Migração, Instalação e Configuração do ADOBE® CONNECT™ 8

Conteúdo

Capítulo 1: Preparação para migração, instalação e configuração

As técnicas que você usa para instalar o Adobe® Connect™ dependem do tipo de instalação que você está realizando.

- Se você estiver instalando o Adobe Connect pela primeira vez, consulte os requisitos de instalação, configurações compatíveis e a visão geral técnica neste capítulo. Em seguida, consulte "Instalar o Adobe Connect 8" na página 20.
- Se você estiver migrando da versão 7.5 ou 7.5.1 ou 8.0 para 8.0 SP1, consulte as informações a seguir que explicam o que há de novo nesta versão. Em seguida, consulte "Preparação para migração" na página 3.

Requisitos de instalação

Requisitos de hardware, software e usuário

Para conhecer os requisitos do Adobe Connect e do Adobe Connect Edge Server, consulte www.adobe.com/go/learn_cnn_sysreqs_br.

Requisitos de porta

A tabela a seguir descreve as portas nas quais os usuários devem poder estabelecer conexões TCP.

Número	Endereço de ligação	Acesso	Protocolo
80	*/Qualquer adaptador	Público	HTTP, RTMP
443	*/Qualquer adaptador	Público	HTTPS, RTMPS
1935	*/Qualquer adaptador	Público	RTMP

Nota: *O RTMP (Real-Time Messaging Protocol) é um protocolo da Adobe.*

A tabela a seguir descreve as portas abertas dentro de um cluster. Cada servidor Adobe Connect em um cluster deve poder estabelecer conexões TCP com todos os outros servidores do cluster nessas portas.

Nota: *Essas portas não devem ser abertas ao público, mesmo se você não estiver usando um cluster.*

Número	Porta de origem	Endereço de ligação	Acesso	Protocolo
8506	Qualquer	*/Qualquer adaptador	Privado	RTMP
8507	Qualquer	*/Qualquer adaptador	Privado	HTTP

Cada servidor Adobe Connect de um cluster deve poder estabelecer uma conexão TCP com o servidor de banco de dados na seguinte porta:

Número	Porta de origem	Acesso	Protocolo
1433	Qualquer	Privado	TSQL

A tabela a seguir descreve as portas do servidor que o Adobe Connect usa para se comunicar internamente. Essas portas não devem estar em uso por qualquer outro processo ou programa em um servidor que hospedar o Adobe Connect, pois a inicialização deste pode falhar.

Número	Endereço de ligação	Acesso	Protocolo
1111	127.0.0.1	Interno	RTMP
2909	127.0.0.1	Interno	RMI
4111	*/Qualquer adaptador	Interno	JMX
8510	127.0.0.1	Interno	HTTP

Se você estiver instalando um adaptador de telefonia personalizado ou integrado, cada servidor do Adobe Connect em um cluster deverá ter a seguinte porta disponível:

Número	Endereço de ligação	Acesso	Protocolo
9080	*/Qualquer adaptador	Público se estiver usando o adaptador de telefonia InterCall; caso contrário, interno	HTTP

Alguns adaptadores de telefonia integrados exigem acesso a portas específicas, além das portas relacionadas nas tabelas acima. Essas portas são relacionadas nas informações para cada adaptador; consulte “Preparação para instalar adaptadores de telefonia integrados” na página 15.

Para obter mais informações sobre portas do Flash Media Gateway, consulte “Protocolos e portas do Flash Media Gateway” na página 43.

Configurações com suporte

Configurações com suporte do banco de dados do servidor

O Adobe Connect usa um banco de dados para armazenar informações sobre usuários e conteúdo. Em seguida, o instalador do Adobe Connect inclui o Microsoft® SQL Server® 2005 Express Edition. O Adobe Connect também é compatível com o Microsoft SQL Server 2005 Standard Edition e o Microsoft SQL Server 2008. Essas edições do SQL Server não estão incluídas no Adobe Connect.

Veja a seguir as configurações do Adobe Connect e do banco de dados às quais existe suporte:

Servidor único com um mecanismo de banco de dados incorporado Instale o Adobe Connect em um único computador e instale o mecanismo de banco de dados incorporado (incluído no instalador do Adobe Connect) no mesmo computador. O mecanismo de banco de dados incorporado é o Microsoft SQL Server 2005 Express Edition.

Nota: *Essa configuração deve ser usada somente em ambientes de teste e não em ambientes de produção.*

Servidor único com SQL Server Instale o Adobe Connect em um único computador e o Microsoft SQL Server 2005 Standard Edition no mesmo computador.

Servidor único com um banco de dados SQL Server externo Instale o Adobe Connect em um único computador e instale o SQL Server em outro computador.

Servidor único com vários bancos de dados SQL Server externos Instale o Adobe Connect em um único computador e instale o SQL Server em vários computadores (também denominado cluster) externos ao Connect. O Adobe Connect oferece suporte ao espelhamento e agrupamento de bancos de dados SQL Server.

Vários servidores com um banco de dados SQL Server externo Instale o Adobe Connect em vários servidores (também denominado cluster) e instale o SQL Server em outro computador.

Vários servidores com vários bancos de dados SQL Server externos Instale o Adobe Connect em vários servidores (também denominado cluster) e instale o SQL Server em um cluster separado. O Adobe Connect oferece suporte ao espelhamento e agrupamento de bancos de dados SQL Server.

Implantações de Flash Media Gateway com suporte

Implante o Flash Media Gateway para ativar o Universal Voice. Os itens a seguir são implantações com suporte:

Um computador Instale o Adobe Connect, o Flash Media Gateway e o SQL Server no mesmo computador.

Dois computadores Instale o Adobe Connect e o Flash Media Gateway no mesmo computador e o SQL Server em outro computador.

Cluster de computadores Instale cada Adobe Connect Server e Flash Media Gateway em computadores separados.

Mais tópicos da Ajuda

"Opções de conferência de vídeo e áudio do Adobe Connect" na página 14

"Implantação do Universal Voice" na página 42

Servidores de diretório LDAP com suporte

Você pode configurar a autenticação do usuário em relação ao servidor de diretório LDAP de sua organização e importar informações de diretório para o Adobe Connect oriundas do servidor de diretório LDAP da organização. Para obter uma lista dos servidores de diretórios LDAP compatíveis, consulte www.adobe.com/go/learn_cnn_sysreqs_br.

Nota: *Qualquer servidor de diretório LDAP v.3 pode ser integrado ao Adobe Connect. No entanto, somente servidores de diretório testados pela Adobe são suportados.*

Mais tópicos da Ajuda

"Integração com um serviço de diretório" na página 35

Dispositivos de armazenamento de conteúdo com suporte

Você pode configurar o sistema Adobe Connect para armazenar conteúdo nos dispositivos Network Attached Storage (NAS) e Storage Area Network (SAN). Para obter uma lista dos dispositivos NAS e SAN com suporte, consulte www.adobe.com/go/learn_cnn_sysreqs_br.

Mais tópicos da Ajuda

"Configuração do armazenamento compartilhado" na página 52

Preparação para migração

Caminhos de migração

Execute o instalador do Adobe Connect 8.1 para atualizar do Connect Pro 7.5, do Connect 8 para Adobe Connect 8.1. O instalador do Adobe Connect orienta você na atualização.

Para obter mais informações sobre como atualizar, entre em contato com o Suporte da Adobe: www.adobe.com/support/programs/connect.

Fluxo de trabalho para migrar para o Adobe Connect 8

Siga este fluxo de trabalho para migrar para o Adobe Connect 8.1.

1. Teste a migração em um ambiente que não seja de produção.

Convém criar um instantâneo do ambiente de produção atual e testar a migração em um ambiente que não seja de produção antes de migrar para o ambiente de produção. Depois que você tiver migrado com êxito em um ambiente de teste, vá para a etapa 2.

2. Informe os usuários sobre a migração.

Consulte “Informar os usuários sobre a migração” na página 4.

3. (Opcional) Faça backup dos arquivos de configuração e conteúdo.

Consulte “Fazer backup dos arquivos” na página 4.

4. Faça backup do banco de dados.

Consulte “Fazer backup do banco de dados” na página 94.

5. Execute o instalador do Adobe Connect 8.

Consulte “Instalar o Adobe Connect 8” na página 20. O instalador pára os serviços do Adobe Connect e faz o backup dos arquivos existentes, incluindo o arquivo custom.ini.

(Opcional) Colete informações necessárias para instalar um ou mais adaptadores de telefonia integrados.
Consulte “Preparação para instalar adaptadores de telefonia integrados” na página 15.

Verifique a instalação.
Consulte “Verificar a instalação” na página 23.

Informar os usuários sobre a migração

Assim como em qualquer atualização de software, principalmente aquelas que afetam um grupo de trabalho, a comunicação e o planejamento são importantes. Antes de começar a migrar ou adicionar módulos ao Adobe Connect, a Adobe sugere que você execute este procedimento:

- Aloque tempo suficiente para garantir o êxito da migração. A atualização deve se encaixar no seu período normal de manutenção.
- Avise aos usuários com antecedência de que eles não poderão usar o Adobe Connect durante a migração.
- Avise aos usuários sobre quais tipos de alterações eles podem esperar (como novos recursos ou melhora no desempenho) após a migração. Para obter mais informações sobre o que há de novo, consulte www.adobe.com/br/products/adobeconnect.html.

Fazer backup dos arquivos

O instalador cria cópias de backup dos diretórios appserv e comserv e do arquivo custom.ini e instala novas versões. O instalador não apaga nem substitui o diretório de conteúdo.

Você também pode fazer backup desses diretórios e arquivos.

Atualização do SQL Server 2005 Express Edition

Siga este fluxo de trabalho para migrar do banco de dados incorporado para o SQL Server 2005 Standard Edition ou SQL Server 2008 em um computador diferente.

Nota: *Você pode realizar essa migração quando migrar para o Adobe Connect. Também pode fazê-la a qualquer momento após a instalação do Adobe Connect.*

1. Instale o SQL Server em um computador diferente do que hospeda o Adobe Connect.

Siga as instruções fornecidas pela Microsoft para instalar o SQL Server.

2. Faça backup do banco de dados incorporado (SQL Server 2005 Express Edition).

Consulte “Fazer backup do banco de dados” na página 94.

3. Copie o arquivo .bak do computador que hospeda o Adobe Connect para o computador que hospeda o SQL Server.

Ao fazer o backup do SQL Server Expression Edition, é criado um arquivo chamado *breeze*.bak (onde *breeze* é o nome do banco de dados).

4. Restaure o banco de dados no computador que hospeda o SQL Server.

Para obter mais informações sobre como restaurar o SQL Server, consulte o Microsoft TechNet.

5. Insira as informações do banco de dados do SQL Server no console de gerenciamento de aplicativos no servidor que hospeda o Adobe Connect.

Escolha Iniciar > Programas > Adobe Connect Server > Configurar o Connect Enterprise Server.

Preparação para instalar o Adobe Connect

Visão geral técnica do Adobe Connect

Uma instalação do Adobe Connect consiste em vários componentes: Connect Central Application Server, Adobe® Flash® Media Server, Adobe Connect Presence Service, Flash Media Gateway (Universal Voice), um banco de dados, Adobe Connect Telephony Service e adaptadores de telefonia para conferência de áudio.

O Adobe Connect Central Application Server está integrado em um aplicativo da Web J2EE em execução no mecanismo de servlet Tomcat. Chamado de *servidor de aplicativos*, ele gerencia usuários, grupos, conteúdo por demanda e sessões de clientes. Algumas das tarefas do servidor do aplicativos incluem controle de acesso, segurança, cotas, licenciamento e funções de auditoria e gerenciamento, como criação de clusters, failover e replicação. Ele também transcodifica mídias, incluindo a conversão de Microsoft® PowerPoint e áudio em Adobe® Flash®. O servidor de aplicativos lida com solicitações de reunião e solicitações de transferência de conteúdo (slides, páginas HTTP, arquivos SWF e arquivos no pod de compartilhamento de arquivos) em uma conexão HTTP ou HTTPS.

Determinados componentes do Flash Media Server (FMS), também chamado de *servidor de reunião*, é instalado com o Adobe Connect para lidar com streaming de áudio e vídeo em tempo real, sincronização de dados e apresentação de conteúdo em mídia avançada, o que inclui interações com as reuniões do Adobe Connect, Algumas tarefas do Flash Media Server incluem gravação e reprodução da reunião, temporização da sincronização de áudio e vídeo e transcodificação (a conversão e a compactação de dados para compartilhamento e interação em tempo real na tela). O Flash Media Server também reduz a carga e a latência do servidor pois armazena no cache as páginas, os fluxos e os dados compartilhados acessados com freqüência. O Flash Media Server transmite áudio, vídeo e dados relacionados à reunião através do protocolo de alto desempenho RTMP ou RTMPS da Adobe.

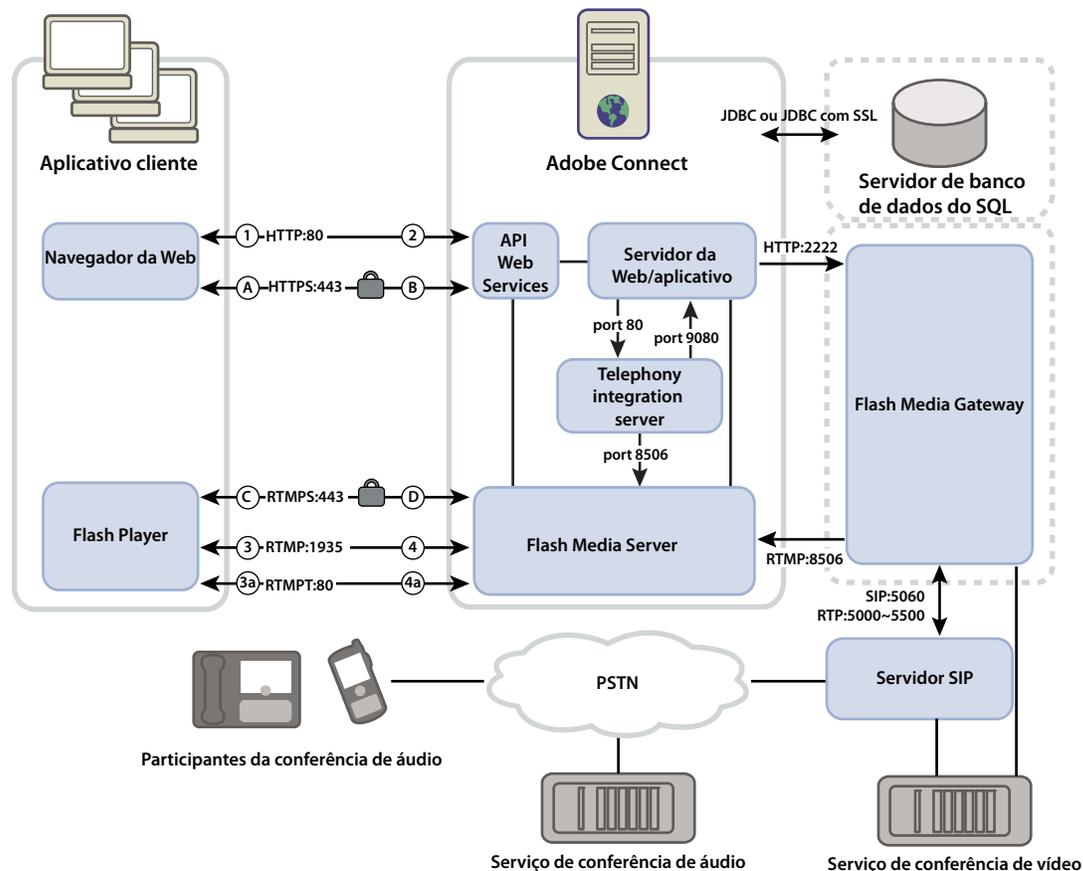
O Adobe Connect Presence Service integra o Adobe Connect com Microsoft® Live Communications Server 2005 e Microsoft® Office Communications Server 2007. Você pode ver a presença de mensagens instantâneas nas salas de reunião do Adobe Connect e enviar mensagens instantâneas para usuários não presentes na sala de reunião. Escolha se deseja instalar o Presence Service durante a instalação.

O Flash Media Gateway integra o Adobe Connect à sua infra-estrutura SIP/RTP. O Flash Media Gateway recebe o áudio de um servidor SIP e o envia para as salas de reuniões do Adobe Connect. O Flash Media Gateway também transmite vídeo e áudio de dispositivos de Conferência de Áudio para o pod Telefonia de Vídeo. Essa solução chama-se Universal Voice.

O Adobe Connect exige um banco de dados para armazenamento persistente de metadados transacionais e de aplicativos, inclusive informações de usuário, grupo, conteúdo e relatórios. Você pode usar o mecanismo de banco de dados incorporado (SQL Server 2005 Express Edition) incluído no instalador do Adobe Connect, ou comprar e instalar o Microsoft SQL Server 2005 Standard Edition.

O Adobe Connect é compatível com vários adaptadores de telefonia para habilitar a conferência de áudio. Você pode escolher instalar um ou mais adaptadores durante o processo de instalação.

Fluxo de dados

O diagrama a seguir ilustra como os dados fluem entre o aplicativo cliente e o Adobe Connect.

Os dados podem fluir por uma conexão criptografada ou não.

Conexão não criptografada

As conexões não criptografadas são criadas em HTTP e RTMP e seguem os caminhos descritos na tabela. Os números na tabela correspondem aos números no diagrama do fluxo de dados.

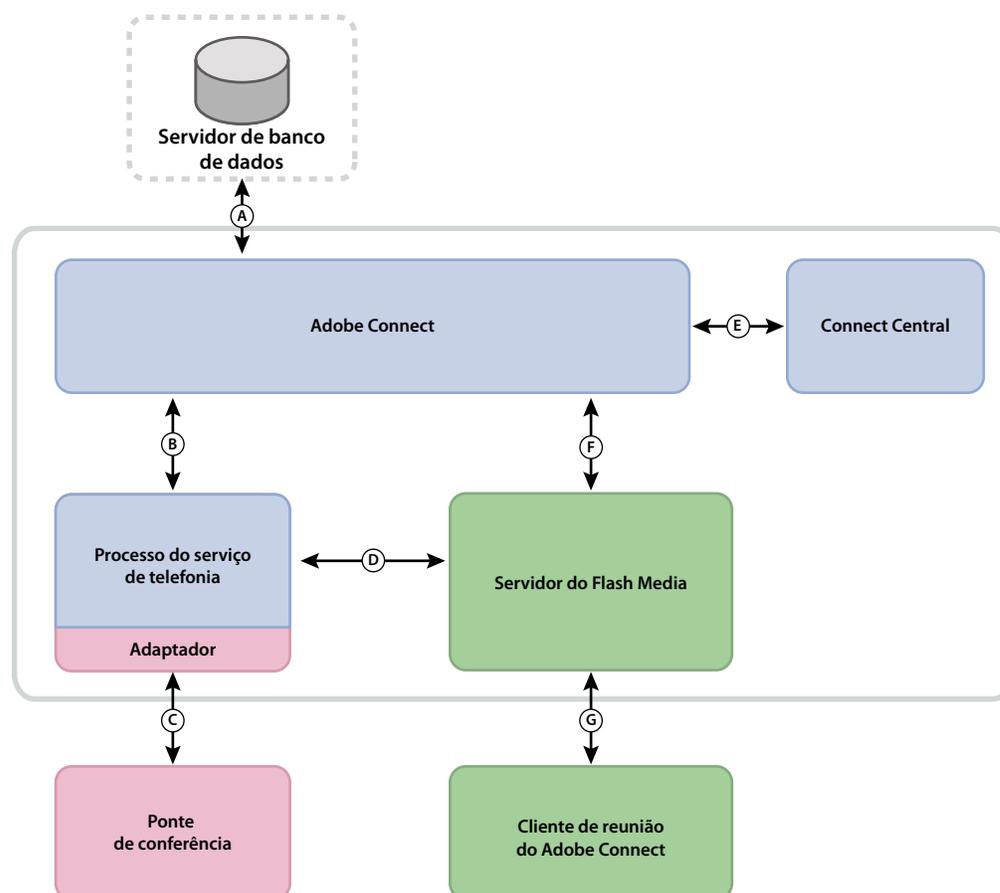
Número	Descrição
1	O navegador da Web do cliente solicita um URL de reunião ou conteúdo em HTTP:80.
2	O servidor Web responde e transfere o conteúdo ou fornece informações ao cliente para ele se conectar à reunião.
3	O cliente Flash Player solicita uma conexão com a reunião em RTMP:1935.
3a	O cliente Flash Player solicita uma conexão com a reunião, mas só pode se conectar em RTMP:80.
4	O Flash Media Server responde e abre uma conexão persistente para o tráfego em streaming do Adobe Connect.
4a	O Flash Media Server responde e abre uma conexão encapsulada para o tráfego em streaming do Adobe Connect.

Conexão criptografada

As conexões criptografadas são criadas em HTTPS e RTMPS e seguem os caminhos descritos na tabela. As letras na tabela correspondem às letras no diagrama do fluxo de dados.

Letra	Descrição
A	O navegador da Web do cliente solicita um URL de reunião ou conteúdo através de uma conexão segura em HTTPS:443.
B	O servidor Web responde e transfere o conteúdo por uma conexão segura ou fornece informações ao cliente para ele se conectar à reunião de forma segura.
C	O cliente Flash Player solicita uma conexão segura com o Flash Media Server em RTMPS:443.
D	O Flash Media Server responde e abre uma conexão segura e duradoura para o tráfego em streaming do Adobe Connect.

Fluxo de dados de telefonia

O diagrama a seguir ilustra como os dados fluem entre os serviços de telefonia e o Adobe Connect.

A. *Persistência.* ***B.*** *Gerenciamento de serviços e failover, conexão de serviço e corretagem de sessão, bem como acesso e provisionamento de dados de usuário.* ***C.*** *Eventos e comandos originais usando APIs de fornecedor proprietário para controle de conferência.* ***D.*** *Eventos e comandos usando chamadas RPC.* ***E.*** *Provisionamento.* ***F.*** *Solicitação de serviço de telefonia.* ***G.*** *Estado e comandos de telefonia.*

Fluxo de trabalho de instalação

As etapas a seguir o ajudarão a projetar, instalar e configurar o sistema Adobe Connect. Algumas etapas exigem que você tome uma decisão e outras exigem que execute uma tarefa. Cada etapa fornece informações sobre a decisão ou a tarefa.

1. Escolha qual banco de dados será utilizado.

Para obter mais informações, consulte "Seleção de um banco de dados" na página 11.

2. Se você optou pelo SQL Server na etapa 1, instale-o.

Para obter mais informações, consulte a documentação do SQL Server.

Nota: *Se você estiver instalando o banco de dados incorporado, você não precisa realizar essa etapa.*

3. (Opcional) Escolha e colete as informações necessárias para instalar adaptadores de telefonia.

Se você estiver instalando um ou mais adaptadores de telefonia integrados, colete as informações que esse instalador exigir. Para obter mais informações, consulte "Instalação de adaptadores de telefonia integrados" na página 12.

4. Instale o Adobe Connect em um único servidor.

Durante a instalação do Adobe Connect 8, você também pode instalar o mecanismo de banco de dados integrado, um ou mais adaptadores de telefonia, Flash Media Gateway (Universal Voice) e o Presence Server. Consulte "Instalar o Adobe Connect 8" na página 20.

5. Verifique se o Adobe Connect está instalado corretamente.

Para obter mais informações, consulte "Verificar a instalação" na página 23.

6. Implante o Adobe Connect.

Para obter mais informações, consulte "Implantação do Adobe Connect" na página 28.

7. (Opcional) Integre o Adobe Connect à sua infra-estrutura.

Há muitas possibilidades para integrar o Adobe Connect à infra-estrutura existente da sua organização. Convém verificar se o Adobe Connect está funcionando depois de configurar cada um desses recursos.

Integrar a um provedor SIP Integre o Adobe Connect com o provedor SIP da sua organização ou provedor SIP terceirizado (também chamado de *provedor VoIP*) para fornecer uma conferência de áudio contínua. Consulte "Implantação do Universal Voice" na página 42.

Integrar ao diretório LDAP Integre o Adobe Connect ao servidor de diretório LDAP da sua organização para que você não precise gerenciar vários diretórios de usuário. Consulte "Integração com um serviço de diretório" na página 35.

Configurar SSL Conduza todas as comunicações do Adobe Connect de forma segura. Consulte "SSL (secure sockets layer)" na página 73.

Armazenar conteúdo em dispositivos NAS/SAN Use dispositivos de rede para compartilhar as tarefas de armazenamento de conteúdo. Consulte "Configuração do armazenamento compartilhado" na página 52.

Integrar ao Live Communications Server e ao Office Communications Server Integre a um servidor de comunicação para permitir que os hosts de reunião vejam a presença para mensagens instantâneas dos convidados em uma sala de reuniões. Os hosts de reunião também podem enviar mensagens para usuários de mensagens instantâneas a partir de uma sala de reuniões. Consulte "Integração com o Microsoft Live Communications Server 2005 e Microsoft Office Communications Server 2007" na página 59.

Configurar uma infra-estrutura de chave pública Se você tiver feito a integração do Adobe Connect com um servidor de diretório LDAP, adicione uma camada de segurança exigindo certificados de cliente. Consulte "PKI (infra-estrutura de chave pública)" na página 73.

Hospedagem do Adobe Connect Add-in Os usuários podem baixar com facilidade o Adobe Connect Add-in dos servidores da Adobe. No entanto, se a política de segurança da sua organização não permitir downloads externos, você poderá hospedar o add-in em seu próprio servidor e ainda contar com uma ótima experiência de usuário. Consulte "Hospedagem do Adobe Connect Add-in" na página 71.

8. (Opcional) Opte por instalar ou não o Adobe Connect em um cluster.

Para obter mais informações, consulte "Implantação do Adobe Connect em um cluster" na página 10.

9. (Opcional) Decida se você deseja instalar servidores de borda.

Para obter mais informações, consulte "Implantação do Adobe Connect Edge Server" na página 12.

Implantação do Adobe Connect em um cluster

É possível instalar todos os componentes do Adobe Connect, inclusive o banco de dados, em um único servidor, mas esse sistema apresenta melhores resultados para testes, não para produção.

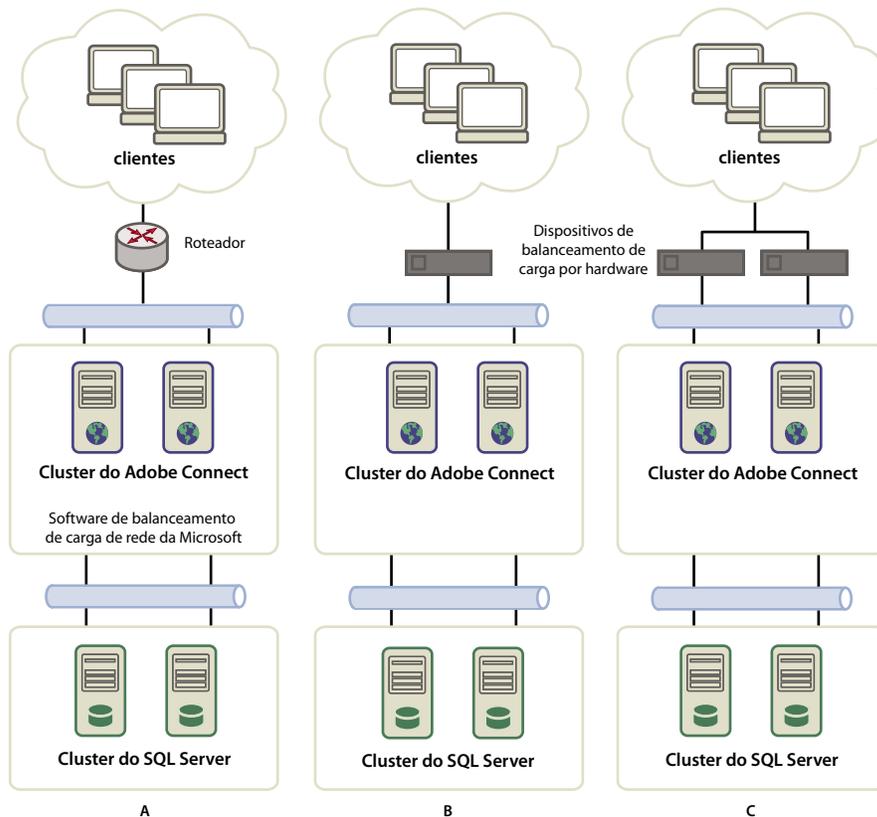
Um grupo de servidores conectados, todos realizando tarefas idênticas, normalmente é chamado de *cluster*. Em um cluster do Adobe Connect, você deve instalar uma cópia idêntica do Adobe Connect em cada servidor no cluster.

Nota: *Quando você instala o Adobe Connect em um cluster, precisa usar o SQL Server 2005 Standard Edition e instalá-lo em um computador separado.*

Se um host do cluster falhar, outro host do cluster assumirá e fará o papel de host na mesma reunião. Você deve utilizar hardware ou software de outras empresas para fornecer o balanceamento de carga para o cluster. Muitas vezes o hardware de balanceamento de carga também pode funcionar como acelerador SSL.

Nota: *No console de gerenciamento de aplicativos, é possível configurar o armazenamento compartilhado, de modo que o conteúdo seja armazenado em dispositivos externos e armazenado em cache no Adobe Connect Server.*

Os sistemas de rede confiáveis são projetados com componentes redundantes; se um componente falhar, outro componente idêntico (*redundante*) poderá assumir o mesmo trabalho. Quando um componente falha e seu substituto assume o controle, diz-se que ocorre *failover*.

O ideal é que todos os componentes do sistema sejam redundantes e não somente o Adobe Connect. Por exemplo, você pode usar vários dispositivos de balanceamento de carga de hardware (como o BIG-IP, da F5 Networks), um cluster de servidores que hospeda o Adobe Connect e bancos de dados do SQL Server em vários computadores externos. Crie seu sistema com o maior número de redundâncias possível e adicione-as gradualmente.

Três opções de criação de cluster
***A.** Cluster com software de balanceamento de carga de rede e dois bancos de dados externos* ***B.** Dois dispositivos de hardware BIG-IP para balanceamento de carga, além de cluster e dois bancos de dados externos* ***C.** Dois dispositivos BIG-IP para balanceamento de carga, além de cluster e dois bancos de dados externos*

Mais tópicos da Ajuda

"Implantar um cluster de servidores Adobe Connect" na página 29

"Configuração do armazenamento compartilhado" na página 52

Seleção de um banco de dados

O Adobe Connect usa um banco de dados para armazenar informações sobre usuários, conteúdo, cursos, reuniões e relatórios. Você pode usar o mecanismo de banco de dados incorporado (incluído no instalador) ou instalar o Microsoft SQL Server 2005 Standard Edition (adquirido separadamente).

***Nota:** O mecanismo de banco de dados incorporado é o Microsoft SQL Server 2005 Express Edition.*

Banco de dados incorporado

O mecanismo de banco de dados incorporado é recomendado para testes e desenvolvimento. Ele usa as mesmas estruturas de dados que o SQL Server 2005 Standard Edition, mas não é tão robusto.

O mecanismo de banco de dados incorporado possui as seguintes limitações:

- Em função das restrições de licenciamento, você precisa instalar o mecanismo de banco de dados incorporado no mesmo computador que o Adobe Connect. O computador deve possuir um único processador.
- 2 GB é o tamanho máximo do banco de dados.

- O mecanismo integrado de banco de dados possui uma interface de linha de comando, e não uma interface gráfica de usuário.

Microsoft SQL Server 2005 Standard Edition

Convém usar o mecanismo Microsoft SQL Server 2005 Standard Edition nos ambientes de produção, pois ele é um sistema de gerenciamento de banco de dados (DBMS) escalonável, projetado para oferecer suporte a um grande número de usuários simultâneos. O SQL Server 2005 Standard Edition também fornece interfaces gráficas para gerenciar e consultar o banco de dados.

Você pode instalar o SQL Server 2005 Standard Edition no mesmo computador do Adobe Connect ou em um computador diferente. Se você os instalar em computadores diferentes, sincronize-os com a mesma origem de tempo. Para obter mais informações, consulte a seguinte nota técnica: www.adobe.com/go/2e86ea67.

Instale o SQL Server em modo de logon misto para usar a autenticação SQL. Configure o banco de dados de modo que não diferencie maiúsculas de minúsculas.

Você deve usar o SQL Server nos seguintes cenários de implantação:

- Instale o banco de dados em um computador que não tenha o Adobe Connect instalado.
- O Adobe Connect é implantado em um cluster.
- O Adobe Connect é instalado em computadores com multiprocessadores com hyperthreading.

Mais tópicos da Ajuda

“Configurações com suporte do banco de dados do servidor” na página 2

Instalação de adaptadores de telefonia integrados

Durante o processo de instalação do Adobe Connect, você tem a opção de instalar um ou mais adaptadores de telefonia.

Cada adaptador requer que você forneça partes específicas de informação. Se você tiver as informações, você poderá configurar o adaptador durante a instalação inicial do Adobe Connect. Se você preferir, você poderá instalar o adaptador sem configurá-lo. Quando você estiver pronto para configurar o adaptador, execute o instalador novamente. Para obter mais informações, consulte “Preparação para instalar adaptadores de telefonia integrados” na página 15.

Implantação do Adobe Connect Edge Server

Quando você implanta o Adobe Connect Edge Server na rede, os clientes se conectam ao servidor de borda e este se conecta ao Adobe Connect (também chamado *servidor de origem*). Essa conexão ocorre de forma transparente; para os usuários, parece que eles estão conectados diretamente ao servidor de origem que hospeda a reunião.

Os servidores de borda fornecem os seguintes benefícios:

Diminuição da latência da rede Os servidores de borda fazem cache do conteúdo por demanda (como reuniões e apresentações gravadas) e dividem fluxos ao vivo, resultando em um tráfego menor para a origem. Os servidores de borda deixam os recursos mais próximos dos clientes.

Segurança Os servidores de borda são uma camada adicional entre a conexão com a Internet do cliente e a origem.

Se sua licença permitir, você poderá instalar e configurar um cluster de servidores de borda. A implantação de servidores de borda em um cluster oferece os seguintes benefícios:

Failover Quando o servidor de borda falha, os clientes são direcionados a outro servidor de borda.

Suporte a grandes eventos Se você precisar de mais de 500 conexões simultâneas para a mesma reunião, um único servidor de borda ficará sem soquetes. O cluster permite mais conexões à mesma reunião.

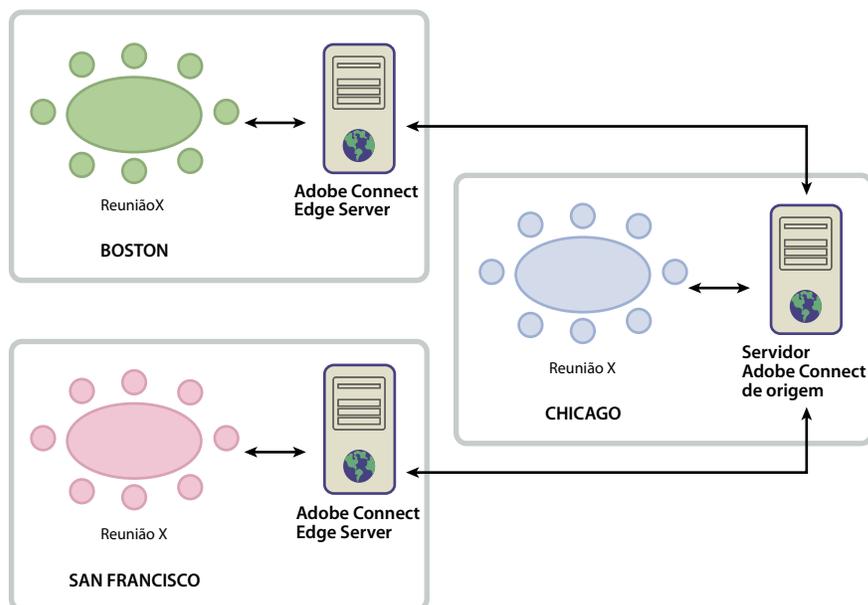
Balanceamento de carga Se você precisar de mais de 100 reuniões simultâneas, um único servidor de borda ficará sem memória. Os servidores de borda podem ser agrupados em cluster por trás do balanceador de carga.

Como funcionam os servidores de borda

Os servidores de borda autenticam usuários e autorizam solicitações de serviços da Web, como o Adobe Connect Meeting, em vez de encaminhar cada solicitação ao servidor de origem e consumir seus recursos nessas tarefas. Se os dados solicitados forem encontrados no cache do servidor de borda, ele retornará os dados ao cliente que os solicitou, sem acionar o Adobe Connect.

Se os dados requisitados não forem encontrados no cache do servidor de borda, este encaminhará a solicitação do cliente para o servidor de origem, no qual o usuário será autenticado e receberá autorização para os serviços. O servidor de origem apresenta os resultados ao servidor de borda solicitante, que entrega os resultados ao cliente requisitante. O servidor de borda também armazena essas informações no cache, no qual outros usuários autenticados podem acessá-las.

Implementação do exemplo do servidor de borda

Veja o seguinte exemplo de implementação de servidor de borda:

Os clientes em Chicago usam a origem localizada em um centro de dados em Chicago. Os servidores de borda em Boston e São Francisco agregam solicitações dos clientes locais e as encaminham para a origem. Os servidores de borda recebem as respostas da origem em Chicago e as transmitem para os clientes em suas zonas.

Mais tópicos da Ajuda

"Instalar o Adobe Connect Edge Server" na página 26

"Implantação do Adobe Connect Edge Server" na página 32

Criação e otimização de um ambiente VMWare

Instalar o Adobe Connect em um VMWare não é diferente de instalá-lo e um computador físico. Para obter informações sobre hardware, software e requisitos de configuração, consulte o documento sobre como executar o Adobe Connect em um ambiente virtual.

Opções de conferência de vídeo e áudio do Adobe Connect

O Adobe Connect é oferece dois tipos de conexão para provedores de conferência de áudio: o Universal Voice e os adaptadores de telefonia integrados. Cada solução oferece benefícios diferentes. É possível configurar uma ou ambas as soluções para um único provedor de conferência de áudio. Você pode configurar quantos provedores de conferência de áudio desejar para uma conta do Adobe Connect.

O **Universal Voice** permite que o Adobe Connect envie e receba áudio de qualquer provedor de conferência de áudio. Você pode gravar áudio junto com a sua conferência da Web e transmitir áudio somente para participantes VoIP.

Use o Universal Voice para integrar dispositivos de telefone de vídeo compatíveis com SIP/H.264. O Adobe Connect é oficialmente compatível com os dispositivos de conferência de vídeo Tandberg 990MXP e Edge 95, embora outros dispositivos Tandberg H.264 também devam funcionar. Para obter mais informações, consulte o site da Tandberg.

A solução Universal Voice usa um componente chamado Flash Media Gateway que é instalado com o Adobe Connect. O Flash Media Gateway recebe o áudio de um servidor SIP e o envia para o Adobe Connect via RTMP. Para usar o Universal Voice é necessário hospedar o seu próprio servidor SIP ou ter uma conta de um provedor SIP. Para obter informações sobre como configurar o Flash Media Gateway, consulte "Implantação do Universal Voice" na página 42.

Depois de ter implantado o Universal Voice, os administradores de conta podem usar o Adobe Connect Central para configurar informações de conferência de áudio. Para obter mais informações, consulte Configurar provedores de áudio para o universal voice.

Adaptadores de telefonia integrados são extensões Java que fazem a comunicação entre o Adobe Connect e provedores de conferência de áudio específicos. Eles fornecem um controle de chamada aprimorado. Você pode instalar um ou mais adaptadores de telefonia ao instalar o Adobe Connect. Para obter mais informações, consulte "Instalação de adaptadores de telefonia integrados" na página 12.

Você também pode usar a API Java de telefonia do Adobe Connect para desenvolver um adaptador de telefonia integrado para um provedor de conferência de áudio.

A tabela a seguir descreve os recursos das duas soluções:

	Provedor de áudio Universal Voice	**Adaptador de telefonia integrado**
Transmitir áudio somente para participantes VoIP	Sim	Não (exceto se o adaptador estiver configurado para o Universal Voice)
Controle de chamadas aprimorado. Por exemplo, silenciar, suspender, entre outros.	Não	Sim
Gravar áudio com a reunião do Adobe Connect	Sim	Sim
Necessita do Flash Media Gateway (fornecido com o instalador do Adobe Connect)	Sim	Não (exceto se o adaptador estiver configurado para o Universal Voice)

Preparação para instalar adaptadores de telefonia integrados

Adaptadores de telefonia integrados fazem a comunicação entre o Adobe Connect e provedores de conferência de áudio específicos. Os adaptadores integrados possuem recursos de chamada avançados que permitem que os hosts e os apresentadores controlem a conferência de áudio na reunião.

Para instalar adaptores de telefone integrados, execute o instalador do Adobe Connect.

Cada adaptador requer que você forneça partes específicas de informação durante a instalação. Para obter mais informações, consulte:

- “Adaptador de telefonia Avaya” na página 15
- “Adaptador de telefonia Cisco Unified MeetingPlace” na página 16
- “Adaptador de telefonia InterCall” na página 17
- “Adaptador de telefonia MeetingOne” na página 18
- “Adaptador de telefonia PGi (ex-Premiere Global) para NA ou EMEA” na página 18

Nota: *Você pode habilitar várias pontes de áudio para o Adobe Connect Server. Hosts de reuniões escolhem qual ponte de áudio usar quando criam uma reunião no Adobe Connect Central. Cada reunião pode ter apenas uma ponte de áudio.*

Adaptador de telefonia Avaya

O adaptador de telefonia Avaya Meeting Exchange™ permite que hosts, apresentadores e participantes de reuniões controlem os recursos da conferência de áudio de salas de reunião do Adobe Connect. Conclua o fluxo de trabalho a seguir para habilitar o adaptador de telefonia.

Trabalho com o suporte ao cliente Avaya

É uma boa ideia envolver o suporte ao cliente Avaya no início do processo de planejamento. Certifique-se de que você tenha as informações de contato do representante da conta Avaya e suporte ao cliente Avaya disponíveis. Contate o suporte Avaya para informá-los que você está instalando e usando o adaptador, e colete informações sobre a ponte.

Nota: *É necessário um contrato de manutenção atual com a Avaya cobrindo a ponte de áudio.*

1 Contate o Suporte ao cliente Avaya.

2 Solicite as seguintes informações:

- O endereço IP da ponte

  A comunicação entre o Adobe Connect e o adaptador de telefonia ocorre através da ponte Avaya.

- Um logon de administração

  Use o logon de administração para configurar e reiniciar a ponte, alterar o número de operadores, adicionar novos usuários e exibir estatísticas.

  Nota: *A Avaya usa um logon adicional para acesso para raiz. A Avaya geralmente não fornece esse logon para clientes. Para operações que exigem acesso de raiz, contate o Suporte ao cliente Avaya.*

- Um logon de acesso a arquivos

  Use o logon de acesso a arquivos para conectar-se ao diretório de arquivos de gravação.

- Uma senha e nome de usuário do Bridge Talk

O Bridge Talk é um aplicativo para gerenciar conferências e chamadores na Ponte de conferência de áudio do Avaya Meeting Exchange. Use o Bridge Talk para determinar se houver um problema com a ponte ou com o adaptador. Você também pode usar este programa para discar para números de telefone; criar, agendar e gerenciar novas conferências; exibir conferências em execução; e monitorar a atividade da ponte. Para obter mais informações, incluindo um Guia do Usuário, consulte www.avaya.com/br.

3 Verifique se você tem acesso ao FTP ao diretório de arquivos de gravação inserindo o seguinte de um prompt de FTP:

```
ftp://bridgeIPAddress
ftp>dcbguest:abc123@machineNameOrIPAddress
ftp>cd /usr3/confrp
ftp>bye
```

Informações necessárias ao instalar

Os itens marcados com asterisco (*) são obrigatórios.

Habilitar discagem Selecione essa opção para habilitar a discagem para todo o sistema. Se você não selecionar essa opção, quaisquer seleções que você fizer para as quatro entradas a seguir serão ignoradas. Se você selecionar essa opção, use as quatro entradas a seguir para especificar como a discagem será implementada.

Habilitar discagem para host Selecione essa opção para permitir que o host da reunião faça a discagem.

Habilitar discagem para apresentador Selecione essa opção para permitir que o apresentador faça a discagem.

Habilitar discagem para participante Selecione essa opção para permitir que os participantes façam a discagem.

Habilitar a caixa de diálogo "Ligar para mim" Se a discagem estiver habilitada, selecione essa opção para exibir a caixa de diálogo "Ligar para mim" para os participantes quando eles ingressarem em uma reunião.

Nome do host do Meeting Exchange* O nome do host ou endereço do servidor Avaya Meeting Exchange.

ID da operadora de telefone* A ID do canal da operadora usada para associação com o servidor do Meeting Exchange.

ID de logon* A ID de logon usada para estabelecer uma conexão com o servidor do Meeting Exchange.

Senha* A senha usada com a ID de logon para conexão com o servidor do Avaya Meeting Exchange.

Diretório de FTP* O diretório de FTP para arquivos de áudio no Avaya Bridge.

Logon de FTP* Nome de usuário do logon de FTP.

Senha de FTP* Senha de logon de FTP.

Número de discagem do Meeting Exchange* Um número de telefone válido discado pelo Adobe Connect para acessar o servidor do Meeting Exchange.

Adaptador de telefonia Cisco Unified MeetingPlace

O adaptador de telefonia MeetingPlace permite que hosts, apresentadores e participantes de reuniões controlem os recursos da conferência de áudio de salas de reunião do Adobe Connect.

Informações necessárias ao instalar

Os itens marcados com asterisco (*) são obrigatórios.

Servidor* do CISCO Unified MeetingPlace URL do Servidor do MeetingPlace

Administrador* do CISCO Unified MeetingPlace A ID que você usa para se conectar ao servidor do MeeetingPlace como um administrador.

Senha* do CISCO Unified MeetingPlace Senha para a conta de administrador do MeetingPlace.

Confirmar senha digite novamente a senha para a conta de administrador do MeetingPlace.

Adaptador de telefonia InterCall

O adaptador de telefonia InterCall permite que hosts, apresentadores e participantes de reuniões controlem os recursos da conferência de áudio de salas de reunião do Adobe Connect. Esse adaptador requer um provedor VoIP ou SIP e Flash Media Gateway (Universal Voice) para a gravação de reuniões. Conclua o fluxo de trabalho a seguir para habilitar o adaptador de telefonia.

Planejamento de implantação

Para implantar o adaptador InterCall, determinadas portas devem estar disponíveis, como mostra a tabela a seguir:

Porta	Descrição
80	O InterCall usa a porta 80 para se comunicar com o Adobe Connect em HTTP. Essa porta deve estar aberta para a comunicação de entrada, a fim de receber retornos do InterCall para o Adobe Connect.
443	O InterCall usa a porta 443 para se comunicar com o Adobe Connect em HTTPS (SSL). Essa porta deve estar aberta para a comunicação de entrada, a fim de receber retornos do InterCall para o Adobe Connect.
8443	O Adobe Connect usa a porta 8443 para se comunicar com o InterCall em HTTPS (SSL). O Adobe Connect usa essa porta para serviços de autorização e CCAPI. Essa porta deve estar aberta para que as mensagens de saída possam ser enviadas do Adobe Connect para o InterCall.
9080	Como mencionado anteriormente, essa porta é necessária para telefonia em geral. No entanto, para o InterCall, ela deve estar aberta também no firewall para cada nó em um cluster.

Informações necessárias ao instalar

Os itens marcados com asterisco (*) são obrigatórios.

Habilitar discagem Selecione essa opção para habilitar a discagem para todo o sistema. Se você não selecionar essa opção, quaisquer seleções que você fizer para as quatro entradas a seguir serão ignoradas. Se você selecionar essa opção, use as quatro entradas a seguir para especificar como a discagem será implementada.

Habilitar discagem para host Selecione essa opção para permitir que o host da reunião faça a discagem.

Habilitar discagem para apresentador Selecione essa opção para permitir que o apresentador faça a discagem.

Habilitar discagem para participante Selecione essa opção para permitir que os participantes façam a discagem.

Habilitar a caixa de diálogo "Ligar para mim" Se a discagem estiver habilitada, selecione essa opção para exibir a caixa de diálogo "Ligar para mim" para os participantes quando eles ingressarem em uma reunião.

Host CCAPI* URL do serviço CCAPI InterCall

Host de autenticação CCAPI* URL do serviço de autorização CCAPI InterCall.

URL de retorno de chamada de cliente* URL de retorno de chamada usada pelo serviço InterCall para retornar a chamada para o Adobe Connect. Essa URL deve estar acessível publicamente.

Token do aplicativo* Valor usado para identificar sua conexão com o serviço de áudio InterCall.

Códigos de país* Lista de códigos de países para os quais o Adobe Connect exibe números de serviço de conferência disponíveis.

Código de país de número gratuito O código de país cujo número de conferência é gratuito; por exemplo, EUA.

Adaptador de telefonia MeetingOne

O adaptador de telefonia MeetingOne permite que hosts, apresentadores e participantes de reuniões controlem os recursos da conferência de áudio de salas de reunião do Adobe Connect.

Informações necessárias ao instalar

Os itens marcados com asterisco (*) são obrigatórios.

Habilitar discagem Selecione essa opção para habilitar a discagem para todo o sistema. Se você não selecionar essa opção, quaisquer seleções que você fizer para as quatro entradas a seguir serão ignoradas. Se você selecionar essa opção, use as quatro entradas a seguir para especificar como a discagem será implementada.

Habilitar discagem para host Selecione essa opção para permitir que o host da reunião faça a discagem.

Habilitar discagem para apresentador Selecione essa opção para permitir que o apresentador faça a discagem.

Habilitar discagem para participante Selecione essa opção para permitir que os participantes façam a discagem.

Habilitar a caixa de diálogo "Ligar para mim" Se a discagem estiver habilitada, selecione essa opção para exibir a caixa de diálogo "Ligar para mim" para os participantes quando eles ingressarem em uma reunião.

URL API MeetingOne* URL do serviço API de conferência de áudio MeetingOne.

SSH Especifica se o download SSH de gravações está habilitado.

Login* do Telephony API Server A ID que você usa para o serviço de API da conferência de áudio do MeetingOne.

Senha* do Telephony API Server Senha da conta do administrador.

Confirmar senha digite novamente a senha para a conta de administrador do MeetingPlace.

Adaptador de telefonia PGi (ex-Premiere Global) para NA ou EMEA

O adaptador de telefonia PGi permite que hosts, apresentadores e participantes de reuniões controlem os recursos da conferência de áudio de salas de reunião do Adobe Connect. As informações nesta seção aplicam-se a adaptadores PGi para NA e EMEA.

Informações necessárias ao instalar

Os itens marcados com asterisco (*) são obrigatórios.

Habilitar discagem Selecione essa opção para habilitar a discagem para todo o sistema. Se você não selecionar essa opção, quaisquer seleções que você fizer para as quatro entradas a seguir serão ignoradas. Se você selecionar essa opção, use as quatro entradas a seguir para especificar como a discagem será implementada.

Habilitar discagem para host Selecione essa opção para permitir que o host da reunião faça a discagem.

Habilitar discagem para apresentador Selecione essa opção para permitir que o apresentador faça a discagem.

Habilitar discagem para participante Selecione essa opção para permitir que os participantes façam a discagem.

Habilitar a caixa de diálogo "Ligar para mim" Se a discagem estiver habilitada, selecione essa opção para exibir a caixa de diálogo "Ligar para mim" para os participantes quando eles ingressarem em uma reunião.

Nota: *Os próximos quatro valores são fornecidos a você pelo PGi.*

Nome do host PGi* O nome do host ou endereço IP do serviço de conferência de áudio do PGi. Para PGi para NA, esse valor geralmente é csaxis.premconf.com. Para PGi para EMEA, esse valor geralmente é euaxis.premconf.com.

Número de porta PGi* O número de porta que o Adobe Connect usa para conectar-se ao serviço de conferência de áudio PGi. Esse valor geralmente é 443.

ID da Web PGi* A ID que você usa para conectar-se ao serviço de conferência de áudio PGi.

Senha PGi* A senha que você usa para conectar-se ao serviço de conferência de áudio PGi.

Logon de download de gravações* O logon que você usa para baixar gravações de áudio do serviço de conferência de áudio PGi.

Senha de download* A senha que você usa com o logon de download de gravações para recuperar gravações do serviço de conferência de áudio PGi.

URL de download A URL que o Adobe Connect usa para baixar gravações do serviço de conferência de áudio PGi. O valor padrão para PGi para NA é https://ww5.premconf.com/audio/. O valor padrão para PGi para EMEA é http://eurecordings.premiereglobal.ie/audio/.

Capítulo 2: Instalação do Adobe Connect

Depois de revisar e coletar as informações necessárias (consulte "Preparação para migração, instalação e configuração" na página 1), você está pronto para instalar o Adobe® Connect™.

Instalar o Adobe Connect 8

Executar o instalador

1 Verifique se seu computador está conectado à Internet.

2 Faça logon no computador como um administrador.

3 Feche todos os aplicativos.

4 Extraia os arquivos do arquivo ESD do Adobe Connect 8 para um local no disco rígido, como C:\Connect_8_ESD.

5 Clique duas vezes para instalar o arquivo install.exe, localizado em *[extract_dir]*\Connect\8.1\Disk1\InstData\VM\install.exe.

6 Selecione um idioma e clique em OK para continuar.

7 Na tela de Introdução, clique em Avançar para continuar.

8 Na tela Contrato de Licença, leia o contrato, marque a opção Aceito os termos do Contrato de licença e clique em Avançar.

9 Execute um dos procedimentos a seguir para selecionar o local da instalação do Adobe Connect:

- Clique em Avançar para aceitar o local de instalação padrão do Adobe Connect (c:\breeze) ou clique em Escolher para selecionar um local diferente.

Nota: *Quando você instalar o Connect 8.1, os arquivos serão instalados em C:\breeze\8.1.0.0. e mencionados como [dir_instalação_raiz] neste documento. No entanto, a pasta de registros e conteúdo é colocada em C:\breeze. Isso significa que instalações subsequentes compartilharão o local de registros e conteúdo, mas arquivos estarão em sua própria pasta de versão C:\breeze\8.x.x.x. Se você estiver migrando de uma versão anterior, todos os arquivos, exceto que será realizado backup do conteúdo e logs.*

- Se você tiver escolhido um local diferente e decidir usar o local padrão, clique em Restaurar pasta padrão.
- Se o Adobe Connect já estiver instalado nesse computador, a tela Atualizar instalação existente será exibida. Marque a caixa de seleção para confirmar que você fez um backup do banco de dados e do diretório raiz do Adobe Connect.

10 Selecione o produto que você deseja instalar e clique em Avançar pata continuar:

- Adobe Connect Server
- Flash Media Gateway (Universal Voice)

Nota: *O Flash Media Gateway requer um provedor SIP/VoIP upstream. Para obter mais informações, consulte "Opções de conferência de vídeo e áudio do Adobe Connect" na página 14.*

- Adaptador de telefonia PGi (para NA)
- Adaptador de telefonia PGi (para EMEA)
- Cisco Unified MeetingPlace

- Adaptador de telefonia Avaya
- Adaptador de telefonia InterCall

Nota: *Se quiser usar o adaptador InterCall, você deverá instalar o Flash Media Gateway.*

- Adaptador de telefonia MeetingOne
- Presence Server

11 Digite o número de série do produto e clique em Avançar.

12 Clique no link para baixar o arquivo de licença da Adobe. Clique em Escolher e procure o arquivo de licença baixado. Clique em Avançar.

13 Se a tela Mecanismo de banco de dados incorporado for exibida, execute um dos procedimentos a seguir:

- Se você planeja instalar um banco de dados em um computador diferente, selecione Não instalar o mecanismo de banco de dados incorporado.
- Para instalar o banco de dados incorporado, selecione Instalar o mecanismo de banco de dados incorporado no seguinte local. Para instalar no local padrão, clique em Avançar. Para selecionar um local diferente, clique em Escolher.

Nota: *Se o instalador detectar que o Microsoft SQL Server já está instalado no computador, o banco de dados não será instalado. Se você estiver migrando e já estiver usando o banco de dados incorporado, o Adobe Connect usará o banco de dados existente. Contudo, o instalador pode detectar uma versão antiga do SQL Server que não funciona com o Adobe Connect. Siga as etapas em* *"Desinstalação do Adobe Connect" na página 27* *e inicie a instalação novamente.*

14 Se você instalou o mecanismo de banco de dados incorporado, digite uma senha forte e clique em Avançar.

15 Defina os valores para as configurações de conexão de banco de dados relacionadas a seguir e clique em Avançar. Os itens marcados com asterisco (*) são obrigatórios.

- **Host*** É o nome de host do computador no qual o banco de dados está instalado. Se tiver instalado o banco de dados incorporado, o valor padrão é `localhost`.
- **Porta*** A porta que o banco de dados usa para se comunicar com o Adobe Connect. O valor padrão é 1433.
- **Nome do banco de dados*** É o nome do banco de dados. O valor padrão é `breeze`.
- **Usuário*** É o nome do usuário do banco de dados. Se tiver instalado o banco de dados incorporado, o valor padrão será `sa`.
- **Senha*** É a senha do usuário do banco de dados. Se tiver instalado o banco de dados incorporado, você poderá definir a senha na etapa anterior.

16 Defina os valores para as configurações de rede relacionadas a seguir e clique em Avançar. Os itens marcados com asterisco (*) são obrigatórios.

- **Nome da conta*** O nome que identifica a conta do Adobe Connect, como "Conta do Adobe Connect".
- **Adobe Connect Host*** Um nome de domínio totalmente qualificado (FQDN) que os clientes usam para se conectar ao Adobe Connect. Por exemplo, se o URL da conta for http://connect.exemplo.com, o valor do Host do Adobe Connect será connect.exemplo.com (sem o http:// à esquerda).
- **Tipo de instalação** Selecione o tipo de instalação como Individual ou Cluster.

17 Defina os valores para as configurações de email relacionadas a seguir e clique em Avançar. Os itens marcados com asterisco (*) são obrigatórios.

- **Host SMTP** É o nome de host do computador no qual o servidor de mensagens SMTP está instalado.
- **Nome de usuário SMTP** O nome de usuário usado para autenticação no host SMTP. Se esse campo ficar em branco, o Adobe Connect tentará enviar emails sem autenticar no servidor SMTP.

- **Senha SMTP** A senha para o nome de usuário SMTP.
- **Email do sistema*** O endereço de email para o qual as mensagens administrativas são enviadas.
- **Email do suporte*** O endereço de email para qual as solicitações de suporte do usuário Adobe Connect são enviadas.
- **Email em Cco** É o endereço de email de uma cópia oculta para o qual todas as notificações de usuários também são enviadas. Esta variável permite o rastreamento administrativo das mensagens de email enviadas por meio do Adobe Connect, sem divulgar endereços de email internos.

18 Digite os valores para as configurações de armazenamento compartilhado relacionadas a seguir e clique em Avançar.

- **Armazenamento compartilhado** É o volume e o diretório de um servidor externo nos quais o conteúdo é armazenado, por exemplo, \\volume\diretório. Se quiser armazenar o conteúdo em vários volumes, separe-os com ponto-e-vírgula (;). Antes de configurar este recurso, consulte a seção “Configuração do armazenamento compartilhado” na página 52.
- **Tamanho de armazenamento em cache de conteúdo** Um número inteiro de 1 a 100 que especifica a porcentagem de espaço livre no disco para o armazenamento de conteúdo no Adobe Connect. O cache pode ultrapassar a porcentagem especificada, portanto, é recomendável manter esse valor de 15 a 50. Se você deixar o campo em branco ou se definir o valor como 0, nenhum espaço do cache será usado e o conteúdo será duplicado no Adobe Connect ou em volumes externos. Antes de configurar este recurso, consulte a seção “Configuração do armazenamento compartilhado” na página 52.

19 Se você escolher instalar o Flash Media Gateway, insira as configurações a seguir e clique em avançar. As configurações não têm efeito imediatamente. Quando você clicar em OK para confirmar as configurações, o Adobe Connect poderá reiniciar todos os servidores Flash Media Gateway. As configurações são enviadas para todos os servidores Flash Media Gateway em um cluster.

- **Nome de usuário** O nome de usuário para o perfil do SIP que o servidor Flash Media Gateway usa para criar sessões SIP, por exemplo sipUN1.
- **Senha** A senha para o perfil do SIP que o servidor Flash Media Gateway usa para criar sessões SIP.
- **Endereço SIP** O endereço do servidor SIP para o perfil do SIP que o servidor Flash Media Gateway usa para criar sessões SIP, por exemplo, 10.12.13.14.
- **Host padrão** O host padrão para o perfil do SIP. Esse parâmetro é o endereço do servidor SIP que será usado se o registro no servidor SIP falhar. Geralmente ele é definido com o mesmo valor do Endereço SIP.
- **Limite inferior de porta** O número mais baixo de porta que pode ser usado para dados de áudio RTP. O valor padrão é 5000.
- **Limite superior em porta** O número mais alto de porta que pode ser usado para dados de áudio RTP. O valor padrão é 6000.
- **Expiração de registro** O intervalo, em segundos, no qual o Flash Media Gateway renova seu registro no servidor SIP. O valor padrão é 2.400 segundos (40 minutos).
- **Porta SIP** A porta na qual o servidor do Flash Media Gateway escuta solicitações SIP. O valor padrão é 5060.
- **Registro** Escolha se um servidor Flash Media Gateway deve se registrar no servidor SIP.

20 Preencha os valores solicitados para criar um administrador de conta e clique em Avançar. Os itens marcados com asterisco (*) são obrigatórios.

Cada conta do Adobe Connect precisa no mínimo de um administrador para realizar tarefas no aplicativo da Web Adobe Connect Central. As contas atualizadas já possuem pelo menos um administrador de contas, mas é possível adicionar outro administrador aqui.

21 Preencha as informações solicitadas para quaisquer adaptadores de telefonia que você deseja instalar. Para obter mais informações sobre adaptadores de telefonia, consulte "Instalação de adaptadores de telefonia integrados" na página 12.

Se você não tiver todas as informações necessárias mas quiser instalar o adaptador mesmo assim, selecione Instalar mas não configurar. Quando você estiver pronto para inserir as informações necessárias, execute o instalador novamente.

22 Revise o resumo da pré-instalação. Clique em Anterior para alterar essas configurações. Clique em Instalar para instalar o software.

23 Na tela Inicializando o serviço Adobe Connect, execute um dos seguintes procedimentos e clique em Avançar:

- Selecione Iniciar o Adobe Connect... (recomendado). Escolha abrir o Connect ou o Console de Gerenciamento do Aplicativo.
- Selecione Não inicie o Connect agora.

24 Se você optou por iniciar o Adobe Connect, será exibida uma mensagem que informa que o serviço está sendo iniciado.

25 Clique em Concluído para sair do Instalador.

26 Se você escolher abrir o Connect, o Connect Central será aberto. Se você escolher abrir o Console de Gerenciamento do Aplicativo, ele será aberto.

27 Verifique a instalação.

Siga as instruções na próxima seção para garantir que sua instalação do Adobe Connect 8 esteja configurada e funcionando como esperado.

Verificar a instalação

Execute as tarefas a seguir para confirmar que sua instalação foi realizada com êxito e que todos os componentes padrão estejão funcionando corretamente. Quando você estiver pronto para implantar o Adobe Connect, consulte "Implantação e configuração do Adobe Connect" na página 28.

Para alterar as definições de configuração inseridas no instalador, use o Console de Gerenciamento do Aplicativo. Escolha Iniciar > Programas > Adobe Connect Server > Configurar o Connect Enterprise Server.

O registro de instalação é criado na pasta *[extract_dir]*\Connect\8.1\Disk1\InstData\VM\. No caso de esse local ser somente leitura, o arquivo de registro será criado em {pasta do usuário}\Local Settings\Temp\AdobeConnect.

Faça logon no Adobe Connect Central

O Adobe Connect Central é um aplicativo da web que permite que você administre o Adobe Connect Server. Se você conseguir fazer logon no Adobe Connect Central, o banco de dados e o Adobe Connect Server poderão se comunicar.

1 Abra um navegador e insira o seguinte URL: http://*[nome do host]*.

Nota: *O parâmetro [nome do host] é o valor definido para o Adobe Connect Host na tela Configurações de Rede no instalador.*

2 Insira o nome de usuário e senha da conta de administrador criada no instalador.

Nota: *Depois de criar usuários adicionais, você poderá fazer logon no Adobe Connect Central com qualquer conta de usuário.*

Verifique se os serviços do Adobe Connect são iniciados

O Adobe Connect Server é executado como um dos serviços Windows a seguir:

- Adobe Connect Presence Server
- Adobe Connect Service
- Adobe Connect Telephony Service
- Flash Media Administration Server
- Flash Media Gateway
- Flash Media Server (FMS)

Mais tópicos da Ajuda

"Iniciar e parar os servidores" na página 81

Verificar se é possível enviar notificações por email

Se você não tiver inserido um valor no campo Host SMTP no Instalador, o Adobe Connect não poderá enviar notificações por email. Se você tiver inserido um Host SMTP, execute um dos procedimentos a seguir para verificar se o Adobe Connect pode enviar notificações por email:

1 Clique na guia Administração, na guia inicial do Adobe Connect Central.

2 Clique na guia Usuários e grupos.

3 Clique em Novo usuário.

4 Na página Informações do novo usuário, digite as informações necessárias. Uma lista parcial das opções é exibida:

Email Use o endereço de email do novo usuário. Verifique se a opção Enviar as informações da conta, logon e senha do novo usuário por email está selecionada.

Nova senha Crie uma senha de 4 a 16 caracteres.

5 Clique em Avançar para continuar.

6 Na área Editar associação do grupo, selecione um grupo, atribua o usuário ao grupo e clique em Concluir.

7 Aguarde até que o usuário receba a notificação por email.

Se o usuário tiver recebido a notificação, o Adobe Connect estará ativo e você poderá enviar mensagens de email pelo seu servidor de emails.

8 Se o usuário não receber a notificação por email, execute o procedimento a seguir:

a Verifique se o endereço de email é válido.

b Verifique se o email não foi filtrado como spam.

c Verifique se o Adobe Connect foi configurado com um valor válido para o Host SMTP e se o serviço SMTP funciona corretamente fora do Adobe Connect.

d Entre em contato com seu suporte da Adobe em www.adobe.com/support/programs/connect.

Verificar se é possível usar o Adobe Presenter

Para certificar-se de que você consegue usar o Adobe Presenter, publique uma apresentação em PowerPoint para o Adobe Connect para conversão em uma apresentação no formato Flash e, em seguida, exiba-a.

1 Se você ainda não tiver feito isso, instale o Adobe Presenter em uma máquina cliente desktop na qual o PowerPoint já esteja instalado.
2 Inicie o navegador e abra o Adobe Connect Central usando o FQDN de seu Adobe Connect Server (por exemplo, connect.exemplo.com).
3 Clique em Recursos > Introdução.
4 Na página Introdução, clique em Publicar apresentações > Instalar Adobe Presenter.
5 Execute o instalador.
6 Se você não tiver uma apresentação em PowerPoint, crie e salve uma apresentação com um ou dois slides.
7 Para abrir o assistente de publicações do Adobe Connect, selecione Publicar, no menu do Adobe Presenter no PowerPoint.
8 Selecione Connect e insira as informações do servidor.
9 Faça logon informando seu endereço de email e senha e execute as etapas do assistente de publicações. Confirme se você está inscrito no grupo de autores (Administração > Usuários e grupos) do Adobe Connect Central.

Quando você concluir as etapas do assistente de publicações, o Adobe Presenter carregará sua apresentação em PowerPoint para o Adobe Connect, que a converte para o formato Flash.

10 Quando a conversão for concluída, vá para a guia Conteúdo, no Adobe Connect Central, e localize sua apresentação.
11 Abra a apresentação para exibi-la.

Verificar se o Training está funcionando (se habilitado)

Nota: *O Adobe Connect Training é um recurso opcional que precisa ser habilitado na sua licença.*

❖ Vá para a guia Treinamento, no Adobe Connect Central.

Se essa guia estiver visível e puder ser acessada, o Connect Training está funcionando. Confirme se você está inscrito no grupo Gerentes de treinamento (Administração > Usuários e grupos).

Verificar se o Meeting está funcionando (se habilitado)

Nota: *O Adobe Connect Meeting é um recurso opcional que precisa ser habilitado na sua licença.*

Para verificar se o Adobe Connect Meeting está funcionando, você precisa estar inscrito no grupo de hosts da reunião ou no grupo de administradores.

1 Faça logon no Adobe Connect Central como um usuário inscrito no grupo de hosts da reunião ou no grupo de administradores.
2 Clique na guia Reuniões e selecione a opção Nova reunião.
3 Na página Digitar informações da reunião, insira as informações necessárias. No campo Acesso à reunião, selecione a opção Somente usuários registrados e convidados aceitos podem entrar na sala. Clique em Concluir para criar a reunião.
4 Clique no botão Entrar na sala de reuniões.
5 Faça logon para entrar na sala de reuniões como usuário registrado.

6 Se a janela do Adobe Connect Add-in for exibida, siga as instruções de instalação.

Se a sala de reuniões for aberta, o Adobe Connect Meeting estará funcionando.

Verificar se o Events está funcionando (se habilitado)

Nota: *O Adobe Connect Events é um recurso opcional que precisa ser habilitado na sua licença.*

1 Faça logon no Adobe Connect Central como um usuário inscrito no grupo de gerentes do evento ou no grupo de administradores.

2 Vá para a guia Gerenciamento de eventos, no Adobe Connect Central.

Se essa guia estiver visível e puder ser acessada, o Adobe Connect Events estará funcionando.

Instalar o Adobe Connect Edge Server

Siga as etapas abaixo se quiser instalar o Adobe Connect Edge Server.

Executar o instalador

1 Feche todos os aplicativos.

2 Navegue até o local dos arquivos que você extraiu quando instalou o Adobe Connect 8, como C:\Connect_8. Em seguida, clique duas vezes no arquivo [extract-dir]\Adobe Edge Server\edgesetup.exe.

3 Escolha um idioma na caixa de diálogo Selecione o idioma da instalação. Clique em OK para continuar.

4 Na tela de Instalação, clique em Avançar para continuar.

5 Na tela Contrato de Licença, leia o contrato, marque a opção Aceito o contrato e clique em Avançar.

6 Execute um dos procedimentos a seguir:

- Clique em Avançar para aceitar o local de instalação padrão (C:\breeze) ou clique em Procurar para escolher um local diferente e clique em Avançar.
- Se o Adobe Connect Edge Server já estiver instalado nesse computador, a tela Atualizar instalação existente do Adobe Connect Edge Server será exibida. Clique em Avançar.

7 Na tela Escolha a pasta do menu Iniciar, execute um dos procedimentos a seguir:

- Clique em Avançar para aceitar o local padrão dos atalhos do menu Iniciar.
- Clique em Procurar para selecionar um local diferente.

8 Na caixa de diálogo Pronto para instalar, verifique os locais onde o Adobe Connect Edge Server e a pasta do menu Iniciar serão instalados. Clique em Voltar para rever ou alterar essas configurações ou clique em Instalar.

9 Clique em Concluir para sair do programa de instalação do Adobe Connect Edge Server

Mais tópicos da Ajuda

"Implantação do Adobe Connect Edge Server" na página 32

Desinstalação dos servidores

Se você quiser desinstalar os servidores, siga as instruções nesta seção.

Desinstalação do Adobe Connect

Nota: *A desinstalação do Adobe Connect não desinstala o SQL Server.*

1 Selecione Iniciar > Programas > Adobe Connect Server > Desinstalar o Connect Server.

Importante: *A pasta raiz (excluída na etapa a seguir) contém os arquivos custom.ini e config.ini, e os arquivos de conteúdo. Se desejar manter o conteúdo, copie esses arquivos para outro local.*

2 Exclua a pasta raiz Adobe Connect. Por padrão, o local é C:\Breeze. Essa pasta contém as seguintes pastas: 8.1.0.0, registros e conteúdo. O arquivo Adobe_Connect_Install.log está localizado na pasta 8.1.0.0.

3 (Opcional) Desinstale o Microsoft SQL Server. Para obter mais informações, consulte http://msdn.microsoft.com.

Desinstalação do Adobe Connect Edge Server

1 Selecione Iniciar > Configurações > Painel de controle > Adicionar ou remover programas > Adobe Connect Edge Server > Remover.

2 Exclua a pasta raiz Adobe Connect. Por padrão, o local onde a pasta está armazenada é C:\breeze.

Desinstalação do Flash Media Gateway

O Flash Media Gateway é desinstalado quando você desinstalar o Adobe Connect. Você também pode executar o seguinte programa para desinstalar o Flash Media Gateway: Arquivos de Programa\Adobe\Flash Media Gateway\Uninstall_Flash Media Gateway\Uninstall Flash Media Gateway.exe.

Capítulo 3: Implantação e configuração do Adobe Connect

Depois que você instalar o Adobe® Connect™, o Flash Media Gateway ou o Adobe Connect Edge Server e concluir a primeira fase da configuração com o console de gerenciamento de aplicativos, configure quaisquer destes recursos opcionais e implante o servidor.

Use o Console de Gerenciamento de Aplicativos para configurar o Adobe Connect Server

Use o Console de Gerenciamento de Aplicativos para definir as configurações do aplicativo Adobe Connect Server e do serviço de diretório, bem como para ver quais recursos estão habilitados em seu servidor.

Quando você instalar o servidor, o instalador solicitará que você insira as configurações do aplicativo. Depois de instalar o servidor, você poderá usar o Console de Gerenciamento de Aplicativos para editar essas configurações.

Para definir as configurações do serviço de diretório, abra o Console de Gerenciamento de Aplicativos depois de instalar o servidor.

❖ Para abrir o Console de Gerenciamento de Aplicativos, execute uma destas ações:

- Escolha Iniciar > Programas > Adobe Connect Server > Configurar o Connect Enterprise Server.
- Um navegador, abra o seguinte URL: http://localhost:8510/console.

Nota: *Se outro aplicativo estiver sendo executado na porta 80, o console de gerenciamento de aplicativos não poderá ser aberto. Pare o aplicativo que estiver sendo executado na porta 80 e abra novamente o Console de gerenciamento de aplicativos. Para verificar se um aplicativo está em execução na porta 80, abra o prompt de comando e digite* ***netstat -a -n -o | findstr LISTEN | findstr ":80 "****.*

Mais tópicos da Ajuda

"Integração com um serviço de diretório" na página 35

"Implantação do Universal Voice" na página 42

Implantação do Adobe Connect

Implantar o Adobe Connect server

1 No servidor DNS, defina um nome de domínio totalmente qualificado (FQDN) para o Adobe Connect (como connect.minhaempresa.com). Mapeie o nome do domínio para o endereço IP estático do computador que hospeda o Adobe Connect.

2 Se você quiser que o Adobe Connect fique disponível fora da rede, configure as seguintes portas do firewall:

80 A porta padrão para o servidor de aplicativos Adobe Connect. A porta terciária para o servidor de reunião (Flash Media Server).

1935 A porta padrão para o servidor de reunião (Flash Media Server).

443 A porta padrão para SSL. A porta secundária para o servidor de reunião (Flash Media Server).

Nota: *Se o tráfego do Adobe Connect for direcionado por um gateway (com um endereço IP diferente), verifique se o firewall está configurado para aceitar solicitações do endereço IP do gateway.*

Para ajudar a implantar o Adobe Connect, entre em contato com o Suporte da Adobe no site www.adobe.com/support/programs/connect.

Mais tópicos da Ajuda

"Requisitos de porta" na página 1

Implantar um cluster de servidores Adobe Connect

1 Instale e configure o Adobe Connect em um servidor dedicado.

Use o mesmo número de série e arquivo de licença todas as vezes que instalar o Adobe Connect. Não instale o mecanismo de banco de dados incorporado e, se seu armazenamento compartilhado exigir um nome de usuário e senha, não inicie o Adobe Connect a partir do instalador.

2 Se o seu armazenamento compartilhado exigir um nome de usuário e senha, execute o seguinte procedimento para adicioná-los ao Adobe Connect Service:

a Abra o painel de controle de serviços.

b Clique duas vezes no Adobe Connect Service.

c Clique na guia Fazer logon.

d Clique no botão de opção Esta conta e digite o nome de usuário do armazenamento compartilhado na caixa. A sintaxe do nome de usuário é [subdomínio\]nomedeusuário.

e Digite e confirme a senha do armazenamento compartilhado.

f Clique em Aplicar e em OK.

3 Faça o seguinte para iniciar o Adobe Connect:

a No painel de controle de serviços, selecione Flash Media Server (FMS) e clique em Iniciar o serviço.

b No painel de controle de serviços, selecione Adobe Connect Service e clique em Iniciar o serviço.

4 Escolha Iniciar > Programas > Adobe Connect Server > Configurar o Connect Enterprise Server para abrir o console de gerenciamento de aplicativos. Clique em Avançar.

5 Na tela Configurações do banco de dados, digite as informações para o banco de dados do SQL Server e clique em Avançar.

Se a conexão do Adobe Connect com o banco de dados tiver êxito, você verá uma confirmação e as configurações do banco de dados. Clique em Avançar.

6 Na tela Configurações do servidor, execute o seguinte procedimento e clique em Avançar:

a Digite um nome de conta.

b Na caixa Host do Connect , digite o nome do computador que está executando o balanceador de carga.

c Digite um número de porta HTTP. Esse número pode ser 80 ou 8080, dependendo do balanceador de carga.

d Digite o nome externo do nó de cluster.

e Digite o nome do domínio do host SMTP e os endereços de email do sistema e do suporte.

f Se você estiver usando armazenamento compartilhado, digite o caminho até o volume ou volumes (separe os vários volumes com ponto-e-vírgula).

g Digite a porcentagem do servidor Adobe Connect que deseja usar como cache local.

Nota: *O conteúdo é gravado no cache local e no volume de armazenamento compartilhado. O conteúdo é mantido no cache local por 24 horas a contar da última vez em que foi usado. Nessa ocasião, se a porcentagem do cache for excedida, o conteúdo será limpo.*

7 Carregue o arquivo de licença e clique em Avançar.

8 Crie um administrador e clique em Concluir.

9 Repita as etapas de 1 a 8 para cada servidor do cluster.

10 Para configurar o balanceador de carga, execute este procedimento:

a Configure o balanceador de carga para escutar na porta 80.

b Adicione todos os nomes de nó do cluster ao arquivo de configuração do balanceador de carga.

Nota: *Para obter informações detalhadas sobre como configurar o balanceador de carga, consulte a documentação do fornecedor.*

11 Abra o navegador da Web e digite o nome do domínio do balanceador de carga, por exemplo, http://connect.mycompany.com.

Para obter ajuda sobre como implantar um cluster, entre em contato com o Suporte da Adobe no site www.adobe.com/support/programs/connect.

Mais tópicos da Ajuda

"Instalar o Adobe Connect 8" na página 20

"Configuração do armazenamento compartilhado" na página 52

Verificação das operações em um cluster

Quando um computador de um cluster é desligado, o balanceador de carga direciona todas as solicitações HTTP para um outro computador do cluster que esteja ligado.

Quando uma reunião é iniciada, o servidor de aplicativos atribui um host primário e um host secundário para a sala de reuniões, com base na carga da mesma. Quando o host primário é desligado, os clientes são conectados novamente ao host secundário.

É recomendável que você verifique se o conteúdo carregado em um servidor do cluster está sendo replicado nos outros computadores do cluster.

O procedimento a seguir pressupõe que o cluster contém dois computadores, o Computador1 e o Computador2.

Verificação do balanceamento de carga e do failover de reunião

1 Inicie o Adobe Connect nos dois computadores.

a Selecione Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Meeting Server.

b Selecione Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Application Server

2 Faça logon no Adobe Connect Central a partir deste URL:

http://*[nome do host]*

Como *nome do host*, use o valor que você definiu para o campo Host do Connect no console de gerenciamento de aplicativos.

3 Selecione a guia Reuniões e clique no link de uma reunião para entrar na sala de reuniões.

Crie uma nova reunião, se necessário.

4 Pare o Connect no Computador2.

a Selecione Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Application Server

b Selecione Iniciar > Programas > Adobe Connect Server > Parar o Connect Meeting Server.

Se o failover da reunião tiver ocorrido de forma apropriada, o indicador de status da conexão da reunião continuará verde.

5 No Adobe Connect, clique em qualquer guia ou link.

Se o balanceador de carga estiver funcionando, você conseguirá enviar solicitações ao Adobe Connect Central e receber respostas.

Se o cluster tiver mais de dois computadores, execute esse procedimento de inicialização e interrupção dos aplicativos para cada computador do cluster.

Verificar a replicação do conteúdo

1 Inicie o Adobe Connect no Computador1.

a Selecione Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Meeting Server.

b Selecione Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Application Server

2 Pare o Connect no Computador2.

a Selecione Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Application Server

b Selecione Iniciar > Programas > Adobe Connect Server > Parar o Connect Meeting Server.

3 Faça logon no Adobe Connect Central a partir deste URL:

http://*[nome do host]*

Como *nome do host*, digite o valor que você definiu para o campo Host do Connect no console de gerenciamento de aplicativos.

4 Carregue uma imagem JPEG ou outro conteúdo no Adobe Connect do Computador1:

- Confirme se você está inscrito no grupo de Autores. (Se for um administrador de conta, você poderá se adicionar ao grupo de autores do Adobe Connect Central.)
- Clique na guia Conteúdo.
- Clique em Novo conteúdo e siga as instruções exibidas no seu navegador para adicionar o conteúdo.

Após carregar o conteúdo de teste, a página Conteúdo do usuário é exibida com uma lista dos conteúdos que pertenciam a você.

5 Clique no link do conteúdo de teste que você acabou de carregar.

A página Informações do conteúdo é exibida com um URL para você acessar o conteúdo.

6 Anote esse URL; ele será usado na etapa 10.

7 Clique no URL.

8 Ligue o Computador2, aguarde até que o Adobe Connect seja totalmente iniciado e desligue o Computador1.

Se o computador tiver um dispositivo externo de armazenamento, não será necessário esperar o Computador2 ser inicializado para desligar o Computador1, pois o conteúdo solicitado será copiado do dispositivo externo.

9 Feche a janela do navegador na qual o conteúdo de teste estava sendo exibido.

10 Abra uma nova janela do navegador e acesse o URL para exibir o conteúdo de teste.

Se o conteúdo de teste for exibido, a duplicação no Computador2 foi realizada corretamente. Uma janela em branco ou uma mensagem de erro indicam que a duplicação falhou.

Implantação do Adobe Connect Edge Server

Fluxo de trabalho da instalação do Adobe Connect Edge Server

1. Desenhe as zonas do servidor de borda.

Você pode configurar servidores de borda ou clusters de servidores de borda em diferentes locais, ou *zonas*, para alocar e balancear o acesso ao Adobe Connect. Por exemplo, você pode configurar um servidor de borda em São Francisco para os usuários da Costa Oeste e um servidor de borda em Boston para os usuários da Costa Leste.

2. Instalar o Adobe Connect Edge Server

Instale o Adobe Connect Edge Server em todos os computadores de cada zona. Por exemplo, se você tiver um cluster de servidores de borda em uma zona, instale o Adobe Connect Edge Server em todos os computadores do cluster. Consulte “Instalar o Adobe Connect Edge Server” na página 26.

3. Modifique o servidor DNS de cada zona.

Mapeie o FQDN do servidor Adobe Connect de origem para o endereço IP estático do Adobe Connect Edge Server em cada zona. Consulte “Implantação do Adobe Connect Edge Server” na página 32.

4. Configure o servidor de borda.

É necessário adicionar parâmetros de configuração ao arquivo custom.ini em cada Adobe Connect Edge Server. Consulte “Implantação do Adobe Connect Edge Server” na página 32.

5. Configure o servidor de origem.

Você precisa adicionar parâmetros de configuração ao arquivo custom.ini em cada servidor Adobe Connect. Além disso, você deve configurar o Nome externo do servidor de borda no Console de gerenciamento de aplicativos do servidor de origem. Consulte “Implantação do Adobe Connect Edge Server” na página 32.

6. Configure um balanceador de carga.

Se você configurar vários servidores de borda em uma zona, deverá usar um balanceador de carga para balancear a carga entre servidores de borda e configurá-lo para aceitar comunicação externa na porta 80. Os servidores de borda aceitam comunicação externa na porta 8080. Para obter mais informações, consulte a documentação fornecida pelo fabricante do balanceador de carga.

Implantação do Adobe Connect Edge Server

Antes de implantar servidores de borda, você deve executar com sucesso o Adobe Connect e todos os recursos adicionais (como SSL, integração de serviço de diretório, logon único, armazenamento de conteúdo compartilhado etc.).

1 No seu servidor DNS, mapeie o FQDN do servidor de origem para o endereço IP estático do servidor de borda. Se você estiver instalando servidores de borda em várias zonas, repita esta etapa para cada zona.

Nota: *Você também pode usar um arquivo de hosts; caso o faça, todos os clientes devem ter um arquivo de hosts que aponte o endereço IP estático do servidor de borda para o FQDN de servidor de origem.*

2 No Adobe Connect Edge Server, abra o arquivo *[dir_instalação_raiz]* \edgeserver\win32\conf\HttpCache.xml e substitua o nome do computador na tag HostName pelo FQDN do computador do servidor de borda, como por exemplo, borda1.exemplo.com.

```
<!-- The real name of this host. -->
<HostName>edge1.yourcompany.com</HostName>
```

3 No Adobe Connect Edge Server, crie um novo arquivo *[dir_instalação_raiz]*\edgeserver\custom.ini e insira os seguintes parâmetros e valores:

FCS_EDGE_HOST O FQDN do servidor de borda, por exemplo, `FCS_EDGE_HOST=edge1.suaempresa.com`.

FCS_EDGE_REGISTER_HOST O FQDN do servidor de origem do Adobe Connect, por exemplo, `FCS_EDGE_REGISTER_HOST=connect.yourcompany.com`.

FCS_EDGE_CLUSTER_ID Nome do cluster. Cada cluster de servidores de borda precisa ter uma ID exclusiva. Todos os computadores dentro do cluster devem ter a mesma ID. O formato recomendado é *`companyname-clustername`*; por exemplo, `FCS_EDGE_CLUSTER_ID=yourcompany-us`.

Nota: *É preciso configurar esse parâmetro, mesmo que você só esteja implantando um Adobe Connect Edge Server.*

FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT O endereço IP ou o nome do domínio e o número da porta do computador onde o Adobe Connect está instalado, por exemplo, `FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80`. O Adobe Connect Edge Server se conecta com o servidor de origem do Adobe Connect nesse local.

FCS_EDGE_PASSWORD (Opcional) Senha do servidor de borda. Se você definir um valor para esse parâmetro, precisará definir o mesmo valor para todos os servidores de borda e para todos os servidores de origem.

FCS_EDGE_EXPIRY_TIME (Opcional) O número de milissegundos nos quais o servidor de borda deve se registrar na origem antes de expirar em um cluster e o sistema alternar para outro servidor de borda. Comece com o valor padrão, `FCS_EDGE_EXPIRY_TIME=60000`.

FCS_EDGE_REG_INTERVAL (Opcional) Intervalo, em milissegundos, em que o servidor de borda tenta se registrar no servidor de origem. Esse parâmetro determina com que freqüência o servidor de borda fica disponível para o servidor de origem. Comece com o valor padrão, `FCS_EDGE_REG_INTERVAL=30000`.

DEFAULT_FCS_HOSTPORT (Opcional) Para configurar as portas do servidor de borda, adicione a seguinte linha: `DEFAULT_FCS_HOSTPORT=:1935,80,-443`.

O sinal de subtração (-) antes do número 443 designa a porta 443 como a porta segura que recebe somente conexões RTMPS. Se você fizer uma tentativa de solicitação de conexão RTMPS com a porta 1935 ou 80, a conexão falhará. Do mesmo modo, as solicitações de conexão RTMP não seguras à porta 443 falharão.

Nota: *Se o seu servidor de borda usar um acelerador de hardware externo, a porta 443 não precisará ser configurada como porta segura.*

Estes são exemplos de valores para o arquivo config.ini:

```
FCS_EDGE_HOST=edge.yourcompany.com
FCS_EDGE_REGISTER_HOST=connect.yourcompany.com
FCS_EDGE_CLUSTER_ID=yourcompany-us
FCS.HTTPCACHE_BREEZE_SERVER_NORMAL_PORT=connect.yourcompany.com:80
```

4 Reinicie o servidor de borda.

5 No servidor de origem do Adobe Connect, abra o arquivo *[dir_raiz_da_instalação]* \custom.ini em um editor de texto e mapeie o valor do parâmetro `FCS_EDGE_CLUSTER_ID` para uma ID de zona. A sintaxe é `borda.`*`FCS_EDGE_CLUSTER_ID = id-da-zona`*. Mesmo se você só estiver implementando um servidor de borda, será preciso mapear a ID do cluster para uma ID de zona.

Cada cluster de servidores de borda precisa ter uma ID de zona. A ID de zona pode ser qualquer número inteiro positivo maior que 0. Por exemplo, você pode ter três clusters mapeados para as zonas de 1 a 3:

```
edge.yourcompany-us=1
edge.yourcompany-apac=2
edge.yourcompany-emea=3
```

A seguir, veja um exemplo de arquivo custom.ini para o servidor de origem:

```
DB_HOST=localhost
DB_PORT=1433
DB_NAME=breeze
DB_USER=sa
DB_PASSWORD=#V1#4cUsRJ6oeFwZLnQPpS4f0w==
# DEBUG LOGGING SETTINGS
HTTP_TRACE=yes
DB_LOG_ALL_QUERIES=yes
# EDGE SERVER SETTINGS
edge.yourcompany-us=1
```

Nota: *Se você configurar um parâmetro `FCS_EDGE_PASSWORD` no arquivo custom.ini no servidor de borda, defina a mesma senha no arquivo custom.ini no servidor de origem.*

6 Reinicie o servidor de origem.

7 No servidor de origem, abra o Console de gerenciamento de aplicativos (Iniciar > Programas > Adobe Connect Server > Configurar o Connect Enterprise Server). Selecione a guia Configurações do aplicativo, depois Configurações do servidor e, na seção Mapeamentos do host, digite o nome externo do servidor de borda. O nome externo deve ser idêntico ao valor definido para o parâmetro `FCS_EDGE_HOST` no servidor de borda.

8 No servidor de origem, configure o firewall do Windows de forma que os servidores de borda possam acessar a porta 8506.

9 Repita as etapas de 2 a 4 para cada servidor de borda em cada zona.

10 Repita as etapas de 5 a 7 para cada servidor de origem em cada zona.

Para obter ajuda sobre como implantar servidores de borda, entre em contato com o Suporte da Adobe no site www.adobe.com/support/programs/connect.

Mais tópicos da Ajuda

"Implantação do Adobe Connect Edge Server" na página 12

Integração com um serviço de diretório

Visão geral da integração com um serviço de diretório

É possível integrar o Adobe Connect a um serviço de diretório a fim de autenticar usuários com relação a um diretório LDAP e evitar a adição manual de usuários e grupos individuais. As contas de usuário são criadas automaticamente no Adobe Connect por meio de sincronizações manuais ou programadas com o diretório da sua organização.

Para fazer a integração com o Adobe Connect, o servidor de diretório deve usar o protocolo LDAP ou LDAPS. O LDAP é um protocolo cliente-servidor da Internet para busca de informações de contato do usuário em um servidor de diretório compatível com LDAP.

O Adobe Connect se conecta como um cliente LDAP a um diretório LDAP. O Adobe Connect importa usuários e grupos e sincroniza informações sobre esses usuários e grupos com o diretório LDAP. Você também pode configurar o Adobe Connect para autenticar usuários em relação ao diretório LDAP.

Qualquer serviço de diretório compatível com LDAP pode se integrar ao Adobe Connect. Para obter uma lista dos diretórios LDAP certificados, consulte www.adobe.com/go/learn_cnn_sysreqs_br.

Sobre a estrutura de diretório LDAP

Os diretórios LDAP organizam informações segundo o padrão X.500.

Os usuários e grupos do diretório LDAP são chamados de *entrada*. Uma entrada é uma coleção de atributos. Um atributo é formado por um tipo e um ou mais valores. Os tipos usam strings mnemônicas, como `ou` para unidade organizacional ou `cn` para nome comum. Os valores de atributo consistem em informações como número de telefone, endereço de email e fotografia. Para determinar a estrutura do diretório LDAP da sua organização, entre em contato com o administrador LDAP.

Cada entrada possui um *nome distinto* (DN) que descreve o caminho até a entrada por meio de uma estrutura em árvore desde a entrada até a raiz. O DN da entrada no diretório LDAP é a concatenação do nome da entrada (chamado de *nome distinto relativo*, RDN) e dos nomes das entradas anteriores na estrutura em árvore.

A estrutura em árvore pode refletir as localizações geográficas ou os limites departamentais dentro de uma empresa. Por exemplo, se houver uma usuária de nome Alicia Solis no departamento de Garantia da Qualidade (QA) da Acme, Inc. na França, o DN dessa usuária poderá ser o seguinte:

cn=Alicia Solis, ou=QA, c=França, dc=Acme, dc=com

Importação de ramos de diretório

Ao importar usuários e grupos de um diretório LDAP para o Adobe Connect, você deve especificar um caminho para a parte da árvore LDAP usando o DN da seção. Isso especifica o escopo da pesquisa. Por exemplo, você quer importar somente os usuários de determinado grupo dentro da empresa. Para fazer isso, você precisa saber onde estão localizadas as entradas desse grupo na estrutura em árvore do diretório.

Uma técnica comum é usar o domínio da Internet da organização como raiz para a estrutura em árvore. Por exemplo, Acme, Inc. pode usar `dc=com` para especificar o elemento raiz na árvore. O DN que especifica o escritório de vendas de Cingapura para a Acme, Inc. pode ser `ou=Cingapura`, `ou=Marketing`, `ou=Funcionários`, `dc=Acme`, `dc=com` (neste exemplo, `ou` é abreviação de unidade organizacional e `dc` é abreviação de componente do domínio).

Nota: *Nem todos os diretórios LDAP possuem uma única raiz. Nessa situação, você pode importar ramos separados.*

Importação de usuários e grupos

Existem duas formas de estruturar as entradas de usuário e grupo no diretório LDAP: sob o mesmo nó de um ramo ou em ramos diferentes.

Se os usuários e grupos estiverem no mesmo nó no ramo LDAP, as configurações de usuário e grupo para a importação de entradas conterão o mesmo DN do ramo. Isso significa que, quando importar usuários, você precisará usar um filtro para selecionar somente os usuários, e quando importar grupos, será necessário usar um filtro para selecionar somente os grupos.

Se os usuários e os grupos estiverem em diferentes ramos da árvore, use um DN do ramo que selecione o ramo do usuário quando você importar o ramo de usuários e de grupo.

Você também pode importar sub-ramos, importando assim usuários de todos os ramos abaixo de determinado nível. Por exemplo, se você quiser importar todos os funcionários do departamento de vendas, use o seguinte DN do ramo:

```
ou=Sales, dc=Acme, dc=com
```

No entanto, os vendedores podem ser armazenados em sub-ramos. Nesse caso, na tela Mapeamento do perfil do usuário, defina o parâmetro Pesquisa de subárvore como `verdadeiro` para garantir que os usuários sejam importados das subárvores abaixo desse nível na árvore.

Filtragem de entradas selecionadas

Um filtro especifica uma condição que a entrada deve satisfazer para ser selecionada. Isso restringe a seleção de entradas dentro de parte da árvore. Por exemplo, se o filtro especificar `(objectClass=organizationalPerson)`, somente as entradas com o atributo `organizationalPerson` serão selecionadas para importação.

***Nota:** O atributo `objectClass` deve estar presente em todas as entradas do diretório LDAP.*

Usuários e grupos internos e externos

Os usuários e grupos criados diretamente no Adobe Connect, e não importados do diretório LDAP, são chamados de *internos*. Os usuários e grupos importados para o banco de dados do Adobe Connect oriundos de um diretório LDAP são chamados de *externos*.

Para garantir que os grupos importados continuem sincronizados com o diretório LDAP externo, você não pode adicionar usuários e grupos internos a grupos externos. No entanto, você pode adicionar usuários e grupos externos a grupos internos.

Se o valor do logon ou nome do usuário ou grupo importado corresponder ao logon de um usuário ou grupo interno existente, a sincronização dos diretórios alterará o usuário ou o grupo importado de interno para externo e colocará uma advertência no registro de sincronização.

Integração do Adobe Connect a um diretório LDAP

A integração com um serviço de diretório ocorre na guia Configurações do serviço de diretório do console de gerenciamento de aplicativos. Use uma conta de administrador.

Você pode configurar um servidor de diretório para autenticação de usuários e sincronização com LDAP. A configuração pode apontar para um ou vários ramos do serviço de diretório.

1. Abra o console de gerenciamento de aplicativo.

Escolha Iniciar > Programas > Adobe Connect Server > Configurar o Connect Enterprise Server.

2. Digite as configurações de conexão do servidor LDAP.

Selecione a guia Configurações do serviço de diretório. Insira os valores na tela Configurações LDAP > Configurações da conexão e clique em Salvar.

Quando você clica em Salvar, o Adobe Connect testa a conexão LDAP. Se o teste falhar, você verá a seguinte mensagem: Suas configurações foram salvas com êxito, mas não foi possível verificar a conectividade LDAP. Verifique o URL e a porta LDAP.

Campo	Valor padrão	Descrição
URL do servidor LDAP	Sem padrão.	O formato normal é `ldap://`***[nomeservidor:númeroporta]***. Se sua organização usar um servidor LDAP seguro, use `ldaps://`. Se você não especificar uma porta, o Adobe Connect usará a porta LDAP padrão (389) ou a porta LDAPS (636). O LDAPS exige certificados SSL. Se você configurar o Adobe Connect para funcionar em uma floresta do Microsoft Active Directory na qual o Catálogo global esteja ativado, use o Catálogo global (porta padrão: 3268).
Método de autenticação da conexão LDAP	Sem padrão.	O mecanismo de autenticação de credenciais (nome de usuário e senha LDAP) da conta do serviço LDAP do Adobe Connect (direitos administrativos). **Simples** (autenticação padrão – recomendada). **Anônimo** (sem senha – o servidor LDAP precisa ser configurado para permitir logon anônimo). **Compilação MD5** (configure o servidor LDAP para permitir a autenticação Digest).
Nome de usuário da conexão LDAP	Sem padrão.	Logon administrativo no servidor LDAP.
Senha da conexão LDAP	Sem padrão.	Senha administrativa no servidor LDAP.
Tempo limite da consulta LDAP	Sem padrão.	Tempo que pode decorrer antes de a consulta ser cancelada, em segundos. Se você deixar o campo vazio, não haverá tempo limite. Defina o valor como 120.
Limite de tamanho de página de entrada de consulta LDAP	Sem padrão.	O tamanho da página de resultados apresentado pelo servidor LDAP. Se essa caixa estiver em branco ou com um 0, não será utilizado o tamanho de página. Use esse campo para servidores LDAP que tenham configurado um tamanho máximo de resultados. Defina o tamanho da página como o tamanho máximo de resultados para que todos eles sejam recuperados do servidor em várias páginas. Por exemplo, se você tentar integrar um diretório LDAP grande que só possa exibir 1000 usuários e houver 2000 usuários a serem importados, haverá falha da integração. Se você definir Tamanho da página de consulta como 100, os resultados serão apresentados em 20 páginas e todos os usuários serão importados.

Veja a seguir um exemplo de sintaxe LDAP para as configurações de conexão:

```
URL:ldap://ldapserver.mycompany.com:389
UserName:MYCOMPANY\jdoe
Password:password123
Query timeout:120
Authentication mechanism:Simple
Query page size:100
```

3. Mapeie perfis de usuário do Adobe Connect e do diretório LDAP.

Selecione a guia Mapeamento do perfil do usuário, digite os valores e clique em Salvar.

Campo	**Valor padrão**	**Descrição**
Logon	Sem padrão.	O atributo de logon do serviço de diretório.
Nome	Sem padrão.	O atributo de nome do serviço de diretório.
Sobrenome	Sem padrão.	O atributo de sobrenome do serviço de diretório.
Email	Sem padrão.	O atributo de email do serviço de diretório.

Se você tiver definido campos personalizados, eles serão adicionados à tela Mapeamento do perfil do usuário. Este exemplo mapeia um perfil de usuário do Adobe Connect para um perfil de usuário do Active Directory LDAP. Logon de rede é um campo personalizado.

```
Login:mail
FirstName:givenName
LastName:sn
Email:userPrincipalName
NetworkLogin:mail
```

4. (Opcional) Adicione um ramo do usuário.

Clique em Adicionar para agregar informações de usuário de um determinado ramo da sua empresa. Digite os valores nos campos Ramo e Filtro e clique em Salvar.

Se desejar importar usuários de sub-ramos, selecione Verdadeiro no menu Pesquisa de subárvore. Caso contrário, selecione Falso.

Para obter mais informações, consulte`“Sobre a estrutura de diretório LDAP” na página 35.

Campo	**Valor padrão**	**Atributo/notas LDAP**
DN do ramo	Sem padrão.	DN (nome distinto) do nó raiz do ramo. Será exibido um link para o ramo selecionado.
Filtro	Sem padrão.	A string do filtro da consulta.
Pesquisa de subárvore	Verdadeiro	Verdadeiro ou Falso. O valor Verdadeiro inicia uma busca recursiva de todas as subárvores do ramo.

5. Mapeie perfis de grupo do Adobe Connect e do diretório LDAP.

Selecione a guia Mapeamento do perfil do grupo, digite os valores e clique em Salvar.

Nota: *Os perfis de grupo do Adobe Connect não oferecem suporte a campos personalizados.*

Campo	**Valor padrão**	**Atributo/notas LDAP**
Nome do grupo	Sem padrão.	O atributo de nome do grupo do serviço de diretório.
Membro do grupo	Sem padrão.	O atributo de membro do grupo do serviço de diretório.

A seguir está o mapeamento entre os atributos de entrada do grupo LDAP e o perfil do grupo do Adobe Connect:

```
Name:cn
Membership:member
```

6. (Opcional) Adicione um ramo do grupo.

Clique em Adicionar para agregar informações de usuário de um ramo da sua empresa. Digite os valores nos campos Ramo e Filtro e clique em Salvar.

Se você quiser importar grupos de sub-ramos, selecione Verdadeiro no menu Pesquisa de subárvore. Caso contrário, selecione Falso.

Para obter mais informações, consulte`"Sobre a estrutura de diretório LDAP" na página 35.

Campo	Valor padrão	Atributo/notas LDAP
DN do ramo	Sem padrão.	DN (nome distinto) do nó raiz do ramo. Todos os ramos da empresa têm seu próprio atributo LDAP DN. Será exibido um link para o ramo selecionado.
Filtro	Sem padrão.	A string do filtro da consulta.
Pesquisa de subárvore	Verdadeiro	Valor booleano de `verdadeiro` ou `falso`. O valor `verdadeiro` inicia uma busca recursiva de todas as subárvores do ramo.

O exemplo a seguir mostra uma sintaxe LDAP para adicionar um braço da empresa e definir seus grupos:

```
DN:cn=USERS,DC=myteam,DC=mycompany,DC=com
Filter:(objectClass=group)
Subtree search:True
```

7. Insira configurações de autenticação.

Selecione a guia Configurações de autenticação. Se desejar autenticar usuários do Adobe Connect em relação ao serviço de diretório de sua organização, selecione "Ativar autenticação com diretório LDAP". Se você não selecionar essa opção, o Adobe Connect usará a autenticação nativa (credenciais de usuário armazenadas no banco de dados do Adobe Connect.

Se você marcar "Ativar fallback do Connect mediante autenticação com Diretório LDAP malsucedida", o Connect usará a autenticação nativa.

Nota: *Essa opção pode ser útil em caso de falha temporária da conectividade LDAP na rede. No entanto, as credenciais LDAP podem ser diferentes daquelas no banco de dados do Adobe Connect.*

Marque "Criar conta de usuário do Connect mediante autenticação com Diretório LDAP bem-sucedida" para suprir usuários que usam o sistema pela primeira vez no servidor Adobe Connect, caso a autenticação LDAP tenha êxito. Se algum usuário em seu serviço de diretório estiver autorizado a usar o Adobe Connect, deixe essa opção marcada e selecione "Interno" como tipo de usuário. Para obter mais informações, consulte "Usuários e grupos internos e externos" na página 36.

Marque "Ativar inscrição de grupo apenas no primeiro logon" para criar uma ID de logon no Adobe Connect e colocar os usuários em grupos especificados quando os usuários fizerem logon no Acrobat Connect pela primeira vez. Insira os grupos na caixa de nomes de grupo.

8. Programe a sincronização.

Selecione a guia Configurações da sincronização. Na tela Programar configurações, marque a caixa de seleção Ativar sincronização programada para programar sincronizações regulares diárias, semanais ou mensais em um determinado momento. Para obter mais informações, consulte "Práticas recomendadas para sincronização" na página 40.

Você também pode realizar uma sincronização manual na tela Ações de sincronização.

9. Defina uma política de senha e uma política de exclusão.

Selecione a guia Configurações da política, escolha uma Política de configuração de senha e uma Política de exclusão e clique em Salvar. Para obter mais informações sobre a política de senhas, consulte "Gerenciamento de senhas" na página 40.

Nota: *Se você selecionar a opção Excluir usuários e grupos, durante uma sincronização, todos os usuários externos que tiverem sido excluídos do servidor LDAP também serão excluídos do servidor Adobe Connect.*

10. Visualize a sincronização.

Selecione a guia Sincronizar ações. Na seção Visualizar sincronização de diretório, clique em Visualizar. Para obter mais informações, consulte “Práticas recomendadas para sincronização” na página 40.

Gerenciamento de senhas

Se você não ativar a autenticação com o LDAP, precisará escolher como o Adobe Connect deve autenticar os usuários.

Quando o Adobe Connect importar informações de usuário de um diretório externo, ele não importará as senhas de rede. Por isso, implemente outro método para gerenciar senhas de usuários importados para o diretório Adobe Connect.

Notificação de usuários para definir a senha

Na tela Configurações da política da guia Configurações da sincronização, você pode optar por enviar um email a usuários importados com um link que lhes permite definir uma senha.

Definir a senha de um atributo LDAP

Você pode optar por definir uma senha inicial de um usuário importado com o valor de um atributo na entrada do diretório do usuário. Por exemplo, se o diretório LDAP contiver o número de ID do funcionário como campo, você pode definir a senha inicial dos usuários como a ID do funcionário. Depois de os usuários fazerem logon usando essa senha, eles poderão trocá-la.

Práticas recomendadas para sincronização

Como administrador, você pode sincronizar o Adobe Connect com o diretório LDAP externo de duas formas:

- Você pode programar a sincronização de forma que ela ocorra em intervalos regulares.
- Você pode realizar uma sincronização manual que sincronize imediatamente o diretório do Adobe Connect com o diretório LDAP da organização.

Antes de importar usuários e grupos em uma sincronização inicial, é uma boa idéia usar um navegador LDAP para verificar os parâmetros de conexão. Estão disponíveis os seguintes navegadores online: Navegador/Editor LDAP e Administrador LDAP.

Importante: *Não reinicie o servidor LDAP nem execute trabalhos paralelos durante a sincronização. Se você fizer isso, poderá fazer com que usuários ou grupos sejam excluídos do Adobe Connect.*

Sincronizações programadas

Recomendam-se sincronizações programadas, pois elas garantem que o Adobe Connect tenha uma visão atualizada dos usuários e grupos importados do diretório LDAP da organização.

Se você estiver importando um grande número de usuários e grupos, a sincronização inicial poderá consumir recursos significativos. Se esse for o caso, é uma boa idéia programar essa sincronização inicial em um momento fora do pico, como durante a madrugada (você também pode fazer essa sincronização inicial manualmente).

Para configurar uma sincronização programada, use a tela Configurações da sincronização > Programar configurações no console de gerenciamento de aplicativos.

Quando ocorre uma sincronização, o Adobe Connect compara as entradas do diretório LDAP às entradas do diretório Adobe Connect e importa somente aquelas que contiverem pelo menos um campo alterado.

Visualização da sincronização

Antes de importar usuários e grupos em uma sincronização inicial, a Adobe recomenda que você teste seus mapeamentos visualizando a sincronização. Em uma visualização, os usuários e os grupos não são realmente importados, mas apenas registram-se os erros; você pode examinar esses erros para diagnosticar problemas na sincronização.

Para acessar os registros de sincronização, use a tela Registros de sincronização. Cada uma das linhas do registro mostra um evento de sincronização; a sincronização produz pelo menos um evento para cada principal (usuário ou grupo) processado. Se forem gerados erros ou advertências durante a visualização, eles serão colocados em um segundo registro de advertência.

Valores do registro

Os registros de sincronização armazenam valores em formato separado por vírgula. Nas tabelas a seguir, *principal* se refere às entradas de usuário e grupo. São incluídos os seguintes valores nas entradas do registro:

Campo	Descrição
Date	Valor data/hora formatado, com medição de tempo até em milissegundos. O formato é *aaaaMMdd'T'HHmmss.SSS*.
Principal ID	O logon ou nome do grupo.
Principal type	Um único caractere: U para usuário, G para grupo.
Event	Ação tomada ou condição encontrada.
Detail	Informações detalhadas sobre o evento.

A tabela a seguir descreve os diferentes tipos de eventos que podem aparecer nos arquivos de registro de sincronização:

Evento	Descrição	Detalhe
add	O principal foi adicionado ao Adobe Connect.	Pacote XML abreviado que descreve os campos atualizados e usa uma série de pares de tags no formato ***<nome_do_campo>valor</nome_do_campo>*** (por exemplo, `<first-name>José</first-name>`). O nó-pai e os campos não atualizados serão omitidos.
update	O principal é um usuário externo e alguns campos foram atualizados.	

update-members	O principal é um grupo externo e os principais foram adicionados ou removidos da associação ao grupo.	Pacote XML abreviado que descreve os membros adicionados e removidos. O nó-pai é omitido:
		`<add>ID list</add>`
		`<remove>ID list</remove>`
		A lista de ID é uma série de pacotes de `<id>principal ID</id>` nos quais o `principal ID` é uma ID relacionada na coluna ID Principal, como o logon do usuário ou o nome do grupo. Se não houver membros de uma lista de ID, o nó-pai apresentará `<add/>` ou `<remove/>`.

delete	O principal foi excluído do Adobe Connect.	

Evento	Descrição	Detalhe
up-to-date	O principal é um principal externo no Adobe Connect e já está sincronizado com o diretório externo. Não foram feitas alterações.	Um usuário ou grupo criado no Adobe Connect é considerado um principal interno. Usuários ou grupos criados pelo processo de sincronização são considerados principais externos.
make-external	O principal do Adobe Connect é do tipo interno e foi convertido em principal externo.	Este evento permite a sincronização para modificar ou excluir o principal e normalmente é seguido por outro evento que faz um ou o outro. Esse evento é registrado no registro de advertência.
warning	Ocorrência de um evento de nível de advertência.	Mensagem de advertência.
error	Ocorrência de um erro.	Mensagem de exceção de Java.

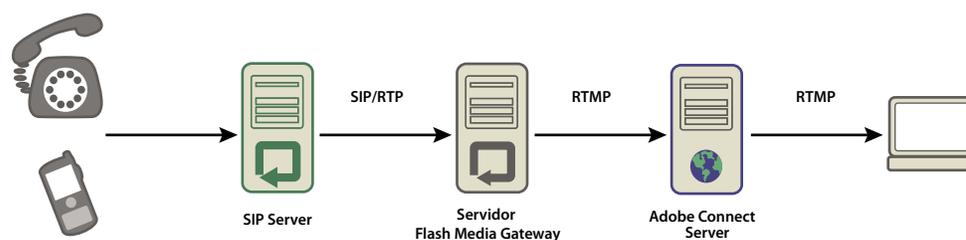
Sobre LDAPS

O Adobe Connect oferece suporte nativo ao protocolo LDAP seguro, *LDAPS*. O servidor de diretório LDAP precisa fornecer conectividade SSL. Para se conectar com segurança a um servidor de diretório LDAP, use o protocolo LDAPS no URL de conexão, como segue: ldaps://*servidorDiretório*:*númeroPorta*.

Implantação do Universal Voice

Fluxo de trabalho da implantação do Universal Voice

Nota: *Para obter uma comparação do Universal Voice e adaptadores de telefonia integrados, consulte "**Opções de conferência de vídeo e áudio do Adobe Connect" na página 14**.*

O Adobe Connect Universal Voice usa um componente intitulado Flash Media Gateway para enviar e receber áudio de um servidor SIP. Instale o Flash Media Gateway e configure-o para estabelecer uma comunicação com um servidor SIP. O servidor SIP pode ser hospedado por terceiros ou por parte da infra-estrutura da sua empresa. Os provedores SIP também são chamados de *provedores VoIP*.

O áudio é transmitido de um telefone e passa por um servidor de conferência de áudio (sem imagem), um servidor SIP e um Flash Media Gateway até chegar à sala de reuniões do Adobe Connect.

Nota: *O Adobe Connect 8 oferece suporte de comunicação bidirecional e dispositivos de vídeo.*

Siga este fluxo de trabalho para implementar a solução Universal Voice:

1 Para instalar e configurar o Universal Voice, é necessário ter o seguinte:

- Adobe Connect 8
- Credenciais de provedor SIP

2 Instale o Flash Media Gateway.

Você pode instalar o Flash Media Gateway no mesmo computador que o Adobe Connect Server ou em um computador dedicado. Você pode implantar o Flash Media Gateway em um único computador ou em um cluster de servidores. O instalador do Flash Media Gateway faz parte do instalador do Adobe Connect Server. Consulte “Executar o instalador” na página 20.

3. Configure o Flash Media Gateway para se conectar com um servidor SIP.
4. Abra as portas. Consulte “Protocolos e portas do Flash Media Gateway” na página 43.

   Se um firewall usar NAT, consulte “Configuração do Flash Media Gateway para comunicação por trás de um firewall que usa o NAT” na página 44.
5. Para instalar o Flash Media Gateway em um cluster de computadores, consulte “Implantar o Flash Media Gateway em um cluster de servidores” na página 47.
6. Para criar uma sequência de discagem e testar a conexão do áudio, consulte Configurar provedores de áudio para o universal voice.
7. Se não conseguir ouvir áudio em uma reunião do Adobe Connect, consulte “Solucionar problemas do Universal Voice” na página 48.

Protocolos e portas do Flash Media Gateway

Nota: *Para exibir um diagrama com o fluxo de dados entre um provedor SIP, o Flash Media Gateway e o Adobe Connect Server, consulte “Fluxo de dados” na página 7.*

O Flash Media Gateway escuta as solicitações do Adobe Connect Central Application Server na seguinte porta:

Número da porta	Endereço de ligação	Protocolo
2222	*/Qualquer adaptador	HTTP

O Flash Media Gateway inicia uma conexão com o Flash Media Server como um cliente RTMP normal. O Flash Media Server escuta o Flash Media Gateway na seguinte porta:

Número da porta	Endereço de ligação	Protocolo
8506	*/Qualquer adaptador	RTMP

O Flash Media Gateway se comunica com o provedor de conferência de áudio pelos protocolos SIP e RTP nas seguintes portas:

Direção	Regra
Flash Media Gateway para Internet	SRC-IP=<Server-IP>, SRC-PORT=5060, DST-IP=ANY, DST-PORT=5060
Internet para Flash Media Gateway	SRC-IP=ANY, SRC-PORT=5060, DST-IP=<Server-IP>, DST-PORT=5060
Flash Media Gateway para Internet	SRC-IP=<Server-IP>, SRC-PORT=5000_TO_6000, DST-IP=ANY, DST-PORT=ANY_HIGH_END
Internet para Flash Media Gateway	SRC-IP=ANY, SRC-PORT=ANY_HIGH_END, DST-IP=<Server-IP>, DST-PORT=5000_TO_6000

Nota: *ANY_HIGH_END significa qualquer porta acima de 1024. O intervalo de portas padrão é 5000-6000. Você pode alterar esses valores no console de gerenciamento de aplicativos.*

Configuração do Flash Media Gateway para comunicação por trás de um firewall que usa o NAT

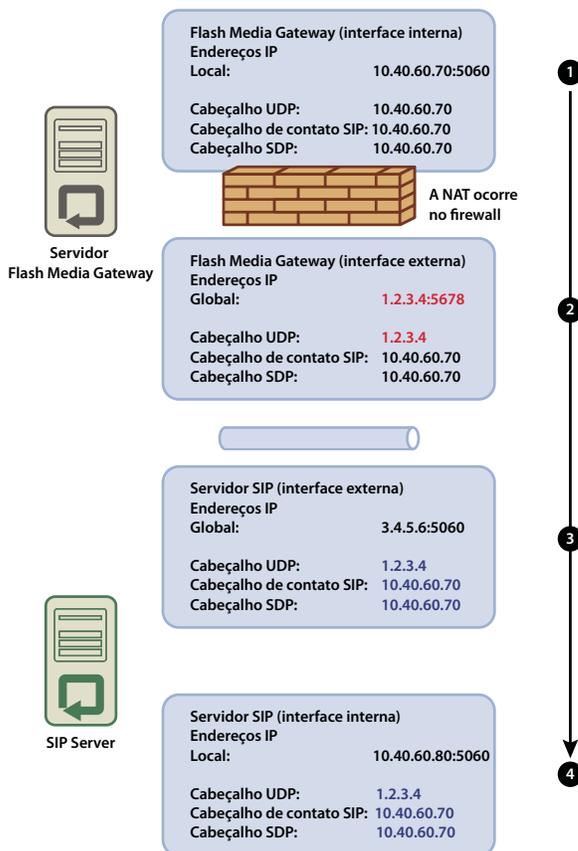
Nota: *Você pode ignorar esta tarefa se o seu firewall para SIP-capable ou SIP-aware. Em alguns casos, o ALG (gateway no nível de aplicativo) para SIP em um firewall pode causar problemas. Se não conseguir estabelecer uma comunicação bem-sucedida usando o ALG, desative o ALG para SIP no firewall e use a técnica descrita nesta seção.*

A tradução de endereço de rede (NAT) é um processo que permite que redes usem menos endereços IP externos e endereços IP internos obscuros. A NAT muda o endereço IP e o número da porta de pacotes no fluxo de saída de uma rede. Os endereços IP internos são alterados para um endereço IP externo. A NAT também tenta direcionar as respostas enviadas para o endereço IP externo a fim de corrigir endereços IP internos.

Quando o Flash Media Gateway estiver atrás de um firewall que usa NAT, talvez ele não consiga receber pacotes do servidor SIP. A NAT altera o endereço IP local e do cabeçalho UDP (origem do pacote) para corresponderem ao endereço IP externo.

O endereço IP do cabeçalho UDP é o mesmo endereço IP externo do Flash Media Gateway. Assim, se o servidor SIP usar o endereço IP do cabeçalho UDP para enviar uma resposta, a resposta encontrará o Flash Media Gateway.

O endereço IP do cabeçalho do contato é o mesmo endereço IP local do Flash Media Gateway. Assim, se o servidor SIP usar o endereço IP do cabeçalho do contato para enviar uma resposta, a resposta não conseguirá encontrar o Flash Media Gateway. O endereço IP local está oculto atrás do firewall e não pode ser visto pelo servidor SIP.

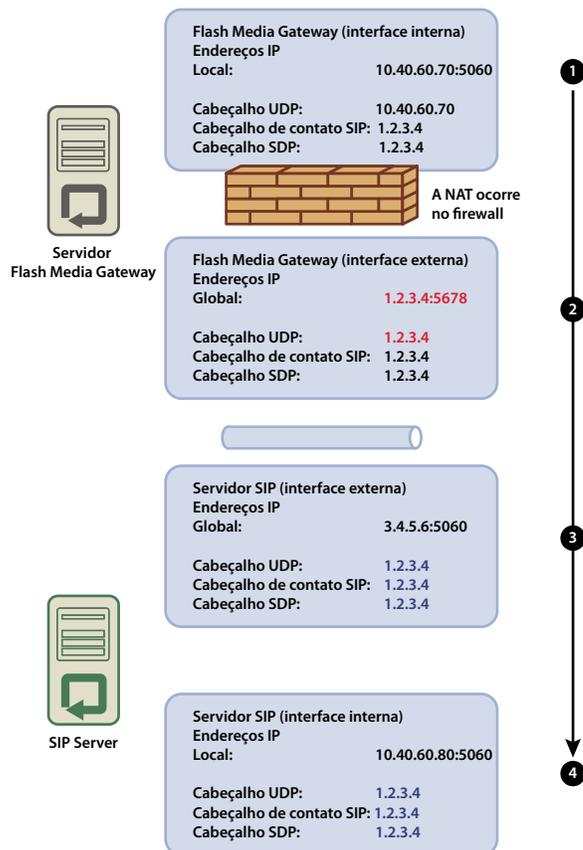
A imagem a seguir mostra como a NAT altera os endereços IP no firewall:

A NAT altera o endereço IP

1 Flash Media Gateway (interface interna). O cabeçalho UDP (endereço IP de origem do pacote) e o endereço IP do cabeçalho do contato do SIP são os mesmos que o endereço IP local.

2 Flash Media Gateway (interface externa). A NAT altera o endereço IP do cabeçalho UDP para o endereço IP global.

3 Servidor SIP (interface externa). O pacote chega à interface global no servidor SIP. Para chegar à interface interna, encaminhe diretamente a porta. Se a porta não for encaminhada, o pacote será perdido e a comunicação falhará.

4 Servidor SIP (interface interna). O pacote é processado quando chega a essa interface. Se o servidor SIP usar o endereço IP do cabeçalho UDP para enviar uma resposta, a resposta chegará ao Flash Media Gateway com sucesso. Se o servidor SIP usar o endereço IP do cabeçalho do contato, a resposta não chegará ao Flash Media Gateway.

A imagem a seguir mostra uma configuração bem-sucedida na qual o endereço IP do cabeçalho do contato do SIP é o mesmo endereço IP externo do Flash Media Gateway. Essa alteração permite que os pacotes sejam roteados de volta para o Flash Media Gateway pelo servidor SIP.

Uma configuração que permite uma comunicação bem-sucedida

Para garantir que o Flash Media Gateway possa receber pacotes de um servidor SIP, execute os procedimentos a seguir:

1 No Flash Media Gateway, abra o arquivo *[dir_instal_raiz]*/conf/sip.xml file em um editor de texto. A pasta de instalação raiz padrão é C:\Arquivos de Programas\Adobe\Flash Media Gateway.)

a Crie uma tag `<globalAddress>` na tag `<Profile>`. Digite o endereço IP externo do Flash Media Gateway, da seguinte forma:

```
...
<Profiles>
    <Profile>
        <profil e I D>   s ipGateway </profileID>
        <userName>141583220 00 </ userName>
        <password></password>
        <displayName> sipGateway </displayName>
        <registrarAddress>8.15.247.100:5060</registrarAddress>
        <doRegister>0</doRegister>
        <defaulthost>8.15.247.100:5060</defaulthost>
        <hostPort> 0 </hostPort>
        <context> sipGatewayContext </context>
        <globalAddress>8.15.247.49</globalAddress>
        <supportedCodecs><codecID> G711u </codecID><codecID> speex </codecID>
    </supportedCodecs>
    </Profile>
</Profiles>
...
```

Em um cluster, cada servidor Flash Media Gateway deve ter um endereço IP externo exclusivo.

Importante: *Se o endereço IP externo for dinâmico, será necessário reconfigurar o Flash Media Gateway sempre que o endereço IP externo mudar.*

b Reinicie o serviço Flash Media Gateway. Consulte "Iniciar e parar o Flash Media Gateway" na página 83.

2 No firewall entre o servidor Flash Media Gateway e o servidor SIP, encaminhe diretamente a porta SIP (5060 por padrão) e todas as portas de voz RTP (5000 - 6000 por padrão) para o servidor Flash Media Gateway. As portas abertas no firewall devem ser as mesmas portas abertas no servidor Flash Media Gateway.

Nota: *Os servidores podem se comunicar sem o encaminhamento de porta. Contudo, as chamadas podem ser desconectadas inesperadamente, principalmente as de longa duração.*

Configurar o nível de log do Flash Media Gateway

Um nível de log elevado pode causar falhas quando o carregamento no Flash Media Gateway for alto. Níveis de log mais elevados gravam mais informações no log. A gravação no log usa energia de processamento e deixa menos energia para a transmissão de áudio. Para melhor desempenho, a Adobe recomenda configurar o nível de log para dados de áudio com 4.

1 Abra o arquivo fmsmg.xml em um editor de texto (por padrão, o arquivo está localizado em C:\Program Files\Adobe\Flash Media Gateway\conf.)

2 Defina o `logLevel` como 4:

```
<logLevel>4</logLevel>
```

3 Reinicie o Flash Media Gateway.

Implantar o Flash Media Gateway em um cluster de servidores

O Flash Media Gateway instalado em um computador com dois processadores pode fazer 100 chamadas simultaneamente. Para processar uma carga maior, aumente o número de processadores ou adicione mais servidores ao cluster Flash Media Gateway.

Para implantar um cluster de servidores, instale o Flash Media Gateway e o Adobe Connect Server em computadores diferentes. Não instale o Adobe Connect Server e o Flash Media Gateway nos mesmos computadores.

Quando você implanta o Flash Media Gateway em um cluster de servidores, o Adobe Connect Server trata do balanceamento de carga e do failover. O Adobe Connect Edge Server não exige uma configuração adicional.

1 Execute o instalador em todos os servidores do cluster e opte por instalar o Flash Media Gateway. Consulte "Executar o instalador" na página 20.

   Nota: *Para obter informações sobre a implantação do Adobe Connect Server em um cluster, consulte "Implantar um cluster de servidores Adobe Connect" na página 29.*

2 Em um servidor Adobe Connect, abra o console de gerenciamento de aplicativos em http://localhost:8510/console.

3 Selecione Configurações do Flash Media Gateway e clique em Adicionar para incluir e configurar outros servidores Flash Media Gateway.

   Nota: *Use o console de gerenciamento de aplicativos em um servidor para inserir os parâmetros de configuração para todos os servidores do cluster. O console de gerenciamento de aplicativos envia as definições da configuração para todos os servidores do cluster.*

Solucionar problemas do Universal Voice

Se não conseguir ouvir o áudio de uma conferência de áudio do Universal Voice em uma sala de reuniões, execute o seguinte procedimento:

1 Verifique se o volume está alto no computador. Se estiver usando fones de ouvido, verifique se eles estão conectados na saída de áudio.

2 Teste a seqüência de discagem. Consulte Testar uma sequência de discagem.

3 Verificar a configuração do Flash Media Gateway:

   a Abra o console de gerenciamento de aplicativos (http://localhost:8510/console) no Adobe Connect Server e clique em Configurações do Flash Media Gateway. O status de cada Flash Media Gateway deve ser "Ativo".

   b Se o status não estiver ativo, abra o arquivo *[dir_instal_raiz]*/custom.ini. Verifique se as seguintes entradas são exibidas:

```
FMG_ADMIN_USER=sa
FMG_ADMIN_PASSWORD=breeze
```

   Se não conseguir ver essas entradas, digite-as e reinicie o Adobe Connect Central Application Server.

4 Entre em contato com seu suporte da Adobe em www.adobe.com/support/programs/connect.

Se você não vir uma opção para adicionar um pod Telefone de vídeo no menu Pods da sala de reunião:

❖ Certifique-se de que o Pod Telefonia de vídeo não esteja desabilitado no Connect Central > Administração >Conformidade e controle.

Implantação de adaptadores de telefonia integrados

Os adaptadores de telefonia integrados são extensões Java que permitem ao Adobe Connect conectar-se a uma ponte de áudio. Você pode instalar qualquer número de adaptadores de telefonia integrados ao instalar o Adobe Connect. Para obter mais informações, consulte "Preparação para instalar adaptadores de telefonia integrados" na página 15.

Depois de instalar um ou mais adaptadores, consulte os tópicos a seguir para verificar e configurar a instalação.

- "Adaptador de telefonia Avaya" na página 49
- "Adaptador de telefonia InterCall" na página 49

- "Adaptador de telefonia MeetingOne" na página 50
- "Adaptador de telefonia PGi (para NA)" na página 51
- "Adaptador de telefonia PGi (para EMEA)" na página 51

Para configurar recursos adicionais de um adaptador após ele ter sido instalado, consulte TechNote no endereço www.adobe.com/go/learn_cnn_customize_adaptor_br.

Adaptador de telefonia Avaya

Conclua as duas tarefas a seguir para confirmar se o adaptador está funcionando como esperado.

Confirmar se a telefonia está habilitada

1. Faça logon no Adobe Connect Central.
2. Clique em Administração > Provedores de áudio.

   Se a telefonia tiver sido habilitada com êxito, você verá o Avaya na lista Provedores. Selecione Avaya e clique em Editar para habilitar ou desabilitar o adaptador para a conta inteira do Adobe Connect.
3. Para adicionar um perfil de áudio Avaya, clique em Meu perfile > Meus perfis de áudio > Novo perfil. Da lista Provedor, selecione Avaya.

   Para obter mais informações, consulte Configurar provedores de áudio para o universal voice.

Testar áudio em uma reunião

❖ Antes de implantar o Adobe Connect em um ambiente de produção, grave pelo menos dois minutos de uma reunião. Veja o arquivo da reunião para confirmar se o áudio foi gravado corretamente.

Desabilitar o adaptador

Se você quiser desabilitar o adaptador Avaya:

1. Pare o Adobe Connect Telephony Service.
2. Abra o arquivo *[dir_instal_raiz]*\telephony-service\conf\telephony-settings.xml.
3. Defina o atributo `enabled` da marca `<telephony-adaptor>` como `false`, como a seguir:

```
<telephony-adaptor id="avaya-adaptor" class-
name="com.macromedia.breeze_ext.telephony.AvayaAdaptor" enabled="false">
```

4. Reinicie o Adobe Connect Telephony Service.

Adaptador de telefonia InterCall

Conclua as duas tarefas a seguir para confirmar se o adaptador está funcionando como esperado.

Confirmar se a telefonia está habilitada

1. Faça logon no Adobe Connect Central.
2. Clique em Administração > Provedores de áudio.

   Se a telefonia tiver sido habilitada com êxito, você verá o InterCall na lista Provedores. Selecione InterCall e clique em Editar para habilitar ou desabilitar o adaptador para a conta inteira do Adobe Connect.
3. Para adicionar um perfil de áudio InterCall, clique em Meu perfile > Meus perfis de áudio > Novo perfil. Da lista Provedor, selecione InterCall.

Para obter mais informações, consulte Configurar provedores de áudio para o universal voice.

Testar áudio em uma reunião

Antes de implantar o Adobe Connect em um ambiente de produção, grave pelo menos dois minutos de uma reunião. Veja o arquivo da reunião para confirmar se o áudio foi gravado corretamente.

Desabilitar o adaptador de telefonia

Se você quiser desabilitar o adaptador InterCall:

1 Pare o Adobe Connect Telephony Service.

2 Abra o arquivo *[dir_instal_raiz]*\TelephonyService\conf\telephony-settings.xml.

3 Defina o atributo `enabled` da marca `<telephony-adaptor>` como `false`, como a seguir:

```
<telephony-adaptor id="intercall-adaptor" class-
name="com.macromedia.breeze_ext.telephony.Intercall.IntercallTelephonyAdaptor"
enabled="false">
```

4 Reinicie o Adobe Connect Telephony Service.

Adaptador de telefonia MeetingOne

Conclua as duas tarefas a seguir para confirmar se o adaptador está funcionando como esperado.

Confirmar se a telefonia está habilitada

1 Faça logon no Adobe Connect Central.

2 Clique em Administração > Provedores de áudio.

Se a telefonia tiver sido habilitada com êxito, você verá o MeetingOne na lista Provedores. Selecione MeetingOne e clique em Editar para habilitar ou desabilitar o adaptador para a conta inteira do Adobe Connect.

3 Para adicionar um perfil de áudio MeetingOne, clique em Meu perfile > Meus perfis de áudio > Novo perfil. Da lista Provedor, selecione MeetingOne.

Para obter mais informações, consulte Configurar provedores de áudio para o universal voice.

Testar áudio em uma reunião

Antes de implantar o Adobe Connect em um ambiente de produção, grave pelo menos dois minutos de uma reunião. Veja o arquivo da reunião para confirmar se o áudio foi gravado corretamente.

Desabilitar o adaptador de telefonia

Se você quiser desabilitar o adaptador MeetingOne:

1 Pare o Adobe Connect Telephony Service.

2 Abra o arquivo *[dir_instal_raiz]*\TelephonyService\conf\telephony-settings.xml.

3 Defina o atributo `enabled` da marca `<telephony-adaptor>` como `false`, como a seguir:

```
<telephony-adaptor id="meetingone-adaptor" class-
name="com.meetingone.adobeconnect.MeetingOneAdobeConnectAdaptor" enabled="false">
```

4 Reinicie o Adobe Connect Telephony Service.

Adaptador de telefonia PGi (para NA)

Conclua as três tarefas a seguir para confirmar se o adaptador está funcionando como esperado.

Configurar nomes de domínio

O Adobe Connect usa HTTP na porta 443 para se comunicar com o PGi. Certifique-se de que o Adobe Connect possa se comunicar com o domínio **csaxis.premconf.com**.

Confirmar se a telefonia está habilitada

1 Faça logon no Adobe Connect Central.

2 Clique em Administração > Provedores de áudio.

   Se a telefonia tiver sido habilitada com êxito, você verá o PGi NA na lista Provedores. Selecione PGi NA e clique em Editar para habilitar ou desabilitar o adaptador para a conta inteira do Adobe Connect.

3 Para adicionar um perfil de áudio PGi NA, clique em Meu perfile > Meus perfis de áudio > Novo perfil. Da lista Provedor, selecione PGi NA.

   Para obter mais informações, consulte Configurar provedores de áudio para o universal voice.

Testar áudio em uma reunião

Antes de implantar o Adobe Connect em um ambiente de produção, grave pelo menos dois minutos de uma reunião. Veja o arquivo da reunião para confirmar se o áudio foi gravado corretamente.

Desabilitar o adaptador de telefonia

Se você quiser desabilitar o adaptador Premiere NA:

1 Abra o arquivo *[dir_instal_raiz]*\TelephonyService\conf\telephony-settings.xml.

2 Defina o atributo `enabled` da marca `<telephony-adaptor>` como `false`, como a seguir:

```
<telephony-adaptor id="premiere-adaptor" class-
name="com.macromedia.breeze_ext.premiere.gateway.PTekGateway" enabled="false">
```

3 Reinicie o Adobe Connect.

Adaptador de telefonia PGi (para EMEA)

Conclua as três tarefas a seguir para confirmar se o adaptador está funcionando como esperado.

Configurar nomes de domínio

O Adobe Connect usa HTTP na porta 443 para comunicar-se com o PGi. Certifique-se de que o Adobe Connect possa se comunicar com o domínio **euaxis.premconf.com**.

Confirmar se a telefonia está habilitada

1 Faça logon no Adobe Connect Central.

2 Clique em Administração > Provedores de áudio.

   Se a telefonia tiver sido habilitada com êxito, você verá o PGi EMEA na lista Provedores. Selecione PGi EMEA e clique em Editar para habilitar ou desabilitar o adaptador para a conta inteira do Adobe Connect.

3 Para adicionar um perfil de áudio PGi EMEA, clique em Meu perfile > Meus perfis de áudio > Novo perfil. Da lista Provedor, selecione PGi EMEA.

Para obter mais informações, consulte Configurar provedores de áudio para o universal voice.

Testar áudio em uma reunião

Antes de implantar o Adobe Connect em um ambiente de produção, grave pelo menos dois minutos de uma reunião. Veja o arquivo da reunião para confirmar se o áudio foi gravado corretamente.

Desabilitar o adaptador de telefonia

Se você quiser desabilitar o adaptador PGi EMEA:

1. Pare o Adobe Connect Telephony Service.
2. Abra o arquivo *[dir_instal_raiz]*\TelephonyService\conf\telephony-settings.xml.
3. Defina o atributo `enabled` da marca `<telephony-adaptor>` como `false`, como a seguir:

```
<telephony-adaptor id="premiere-emea-adaptor" class-
name="com.macromedia.breeze_ext.premiere.gateway.EMEA.PTekGateway" enabled="false">
```

4. Reinicie o Adobe Connect Telephony Service.

Ocultar usuário do Flash Media Gateway na lista de participantes

***Nota:** Essa seção se aplica apenas aos adaptadores de telefonia integrados configurados para o Universal Voice.*

Quando uma sala de reuniões se conecta com o Flash Media Gateway, a conexão é exibida como um usuário na lista de participantes. Para ocultar o usuário do Flash Media Gateway na lista de participantes, configure o número da conferência no arquivo custom.ini. Use o mesmo número para todos os computadores em um cluster. Você pode obter o número da conferência de áudio pelo seu provedor SIP. Ou, se o administrador da sua conta tiver configurado um provedor de áudio no Adobe Connect Central, você poderá encontrar o número na sala de reuniões.

1. Abra o arquivo *[DiretóriodaInstalaçãoRaiz]*\custom.ini em um editor de texto.
2. Adicione o seguinte parâmetro:

```
UV_NUMBER={audio_conference_telephone_number}

// Example:
UV_NUMBER=4155551212
```

3. Salve e feche o arquivo custom.ini.
4. Execute os procedimentos a seguir para reiniciar o servidor:
   a. Clique em Iniciar > Programas > Adobe Connect Server > Parar o Adobe Connect Central Application Server.
   b. Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Adobe Connect Central Application Server.

Configuração do armazenamento compartilhado

Sobre o armazenamento compartilhado

Você pode usar o instalador do console de gerenciamento de aplicativos para configurar o Adobe Connect para que use dispositivos NAS e SAN para gerenciar o armazenamento de conteúdo. Conteúdo é qualquer arquivo publicado no Adobe Connect, como cursos, arquivos SWF, PPT ou PDF e gravações arquivadas.

Veja a seguir possíveis configurações de armazenamento compartilhadas:

- O conteúdo é copiado no dispositivo primário de armazenamento externo e utilizado pela pasta de conteúdo de cada servidor Adobe Connect, conforme necessário. O conteúdo antigo é removido de cada pasta do servidor para dar espaço para novos conteúdos, conforme necessário. Essa configuração libera recursos no servidor de aplicativos, que é especialmente útil em um cluster grande. (digite um valor na caixa Armazenamento compartilhado e na caixa Tamanho do cache de conteúdo).
- O conteúdo é copiado em todos os servidores e no dispositivo primário de armazenamento externo. Essa configuração é recomendada para pequenos clusters, a menos que você tenha uma grande quantidade de conteúdo acessada de forma aleatória (digite um valor na caixa Armazenamento compartilhado; deixe a caixa Tamanho do cache de conteúdo em branco).

Nota: *Se você tiver um cluster do Adobe Connect e não configurar dispositivos de armazenamento compartilhado, o cluster trabalhará em modo de espelhamento completo (o conteúdo publicado no Adobe Connect será copiado em todos os servidores) e o conteúdo nunca será removido automaticamente de nenhum servidor.*

Configurar o armazenamento compartilhado

Se você não tiver configurado o armazenamento compartilhado durante a instalação, você poderá fazê-lo seguindo as instruções nesta seção.

- Se você estiver configurando um armazenamento compartilhado para um servidor Adobe Connect, siga as instruções da primeira tarefa.
- Se você estiver configurando um armazenamento compartilhado para um cluster, siga as instruções da primeira tarefa para um computador do cluster e depois siga as instruções da segunda tarefa para todos os outros computadores do cluster.

Mais tópicos da Ajuda

“Dispositivos de armazenamento de conteúdo com suporte” na página 3

“Implantar um cluster de servidores Adobe Connect” na página 29

Configurar o armazenamento compartilhado

O Adobe Connect deve estar configurado sem armazenamento compartilhado e ser executado em um servidor para que você possa continuar.

1 Configure um volume compartilhado em um dispositivo de armazenamento externo.

A conta na qual o serviço Connect é executado deve ter permissões de leitura e gravação no volume compartilhado.

2 (Opcional) Se você estiver atualizando um servidor Adobe Connect existente para usar volumes de armazenamento compartilhado, será necessário copiar o conteúdo de um dos servidores existente no volume compartilhado.

a Pare o servidor (Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Application Server e Parar o Connect Meeting Server).

b Copie a pasta *[dir_instalação_raiz]*\content\7 no volume compartilhado criado na etapa 1.

Alguns computadores do cluster podem ter conteúdo extra. O Adobe Connect não pode usar esses arquivos, mas você pode copiá-los para o volume compartilhado para fins de arquivamento e, depois, escrever e executar um script que compare o conteúdo de cada computador com o conteúdo do volume compartilhado.

c Inicie o Adobe Connect (Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Meeting Server e Iniciar o Connect Central Application Server).

3 No Adobe Connect Server, selecione Iniciar> Painel de controle> Ferramentas administrativas > Serviços para abrir a janela Serviços. Em seguida, selecione Adobe Connect Service e faça o seguinte:

a Clique com o botão direito do mouse e selecione Propriedades.

b Selecione a guia Logon.

c Selecione Esta conta e, caso o volume compartilhado tenha um nome de usuário e uma senha, digite-os e clique em Aplicar.

4 Reinicie o Adobe Connect (somente servidor de aplicativos).

a Clique em Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Application Server.

b Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Application Server.

5 Abra o console de gerenciamento de aplicativos (Iniciar > Programas > Adobe Connect Server > Configurar o Connect Enterprise Server).

6 Na guia Configurações do aplicativo, selecione a guia Configurações do servidor, role até a seção Configurações de armazenamento compartilhadas e digite um caminho de pasta na caixa Armazenamento compartilhado (por exemplo, **\\volume\diretório**).

Se o dispositivo de armazenamento primário se encher, você poderá adicionar outro dispositivo à posição primária. Separe os caminhos por ponto-e-vírgula (;): **\\volume\diretório;\\volume2\diretório**.

Nota: *A gravação (cópia para a pasta de armazenamento) só é realizada na primeira pasta. A leitura (cópia da pasta de armazenamento) é realizada em seqüência, iniciando com a primeira pasta e até o arquivo ser encontrado.*

7 (Opcional) Para configurar a pasta de conteúdo do Adobe Connect para agir como cache (os arquivos são removidos automaticamente quando é necessário abrir espaço, sendo restaurados mediante solicitação), digite um valor na caixa Tamanho do cache de conteúdo.

O tamanho do cache de conteúdo é uma porcentagem do espaço em disco que é utilizada como cache. A Adobe recomenda definir o valor entre 15 e 50, pois o cache pode crescer muito além do valor definido. O cache só é eliminado depois que o conteúdo exibido expira (24 horas após ter sido exibido pela última vez).

8 Clique em Salvar e feche o console de gerenciamento de aplicativos.

9 Reinicie o Adobe Connect (somente servidor de aplicativos).

a Clique em Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Application Server.

b Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Application Server.

Configurar o armazenamento compartilhado para servidores adicionais em um cluster

1 Instale o Adobe Connect, mas não o inicie. Se o Adobe Connect estiver instalado e em execução, pare-o.

2 No Adobe Connect Server, selecione Iniciar> Painel de controle> Ferramentas administrativas > Serviços para abrir a janela Serviços. Em seguida, selecione Adobe Connect Service e faça o seguinte:

a Clique com o botão direito do mouse e selecione Propriedades.

b Selecione a guia Logon.

c Selecione Esta conta e, caso o volume compartilhado tenha um nome de usuário e uma senha, digite-os e clique em Aplicar.

3 Inicie o Adobe Connect.

a Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Meeting Server.

b Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Application Server.

4 (Opcional) Se você estiver instalando o Adobe Connect pela primeira vez, siga as etapas em "Implantar um cluster de servidores Adobe Connect" na página 29.

5 Clique em Salvar e feche o console de gerenciamento de aplicativos.

Configurar links Ajuda e Recursos

Adição de links de suporte e ajuda ao menu Ajuda

Os Administradores de conta podem adicionar os links Página de status e Página de suporte ao menu Ajuda nas Salas de reunião. Os links são as páginas HTML que você desenvolveu. A Página de status pode fornecer informações sobre os status atual do sistema do Adobe Connect. A Página de suporte pode fornecer informações sobre como obter suporte usando o Adobe Connect. Se você não definir esses links, eles não estarão disponíveis no menu Ajuda.

1 Abra o arquivo *PastadaInstalaçãoRaiz*\custom.ini em um editor de texto.

2 Para editar o link Página de status, defina `STATUS_PAGE = "http://connect.mycompany.com/status.html"`.

3 Para editar o link Página de suporte, defina
`SUPPORT_PAGE="http://connect.mycompany.com/support.html"`.

Os URLs podem ser absolutos ou relativos ao domínio do servidor de reuniões. Inicie URLs absolutos com "http://" ou "https://". Inicie URLs relativos com "/".

4 Faça o seguinte para reiniciar o Adobe Connect:

a Clique em Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Application Server.

b Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Application Server.

Redirecionar os links Recursos do Adobe Connect Central

A home page do Adobe Connect Central tem uma guia Recursos, que fornece links para a página Introdução, Ajuda do Adobe Connect Central, Documentação do Adobe Connect e ConnectUsers.com. Você pode redirecionar esses links para outros locais.

Nota: *Você não pode redirecionar o ConnectUsers.com, pois ele vai para um site.*

1 Abra a página que deseja editar em um editor HTML. Em cada caminho de arquivo, substitua o espaço reservado *lang* pelo código de idioma de duas letras. Por exemplo, o código para inglês é "en".

Página	Local	Anotações
Introdução	appserv/common/help/*lang*/support/startmain.htm	Você pode editar esse arquivo no Adobe Connect Server versão 7 e posteriores.
Ajuda do Adobe Connect Central	appserv/common/help/*lang*/connect/8.0/using/AH_HOME.html	Alterar esse arquivo também mudará o link de Ajuda na parte superior do Adobe Connect Central. Você pode editar esse arquivo no Adobe Connect Server versão 7 e posteriores.
Documentação do Adobe Connect	appserv/common/help/*lang*/go/doc.html	Você pode editar esse arquivo no Adobe Connect Server versão 7.5 e posteriores.

2 Para cada um desses arquivos, insira o seguinte como o conteúdo total do arquivo:

```
<!-- ======================================================================
    This is used by Adobe Connect to redirect to the desired webpage.
    If there is a particular place where you would like users to be sent,
    please customize the URL below.
     ====================================================================== -->
<META HTTP-EQUIV=Refresh CONTENT="0; URL=http://desiredpage.com">
```

3 Edite o valor do atributo URL para o destino de seu conteúdo. A URL pode ser um caminho relativo ou um caminho absoluto.

Por exemplo, para redirecionar o arquivo doc.html para a documentação no servidor de sua organização, você deverá usar a URL http://www.mycompany.com/support/documentation/connectpro.

Configurações de notificação de conta

Definir quando relatórios mensais são enviados

O Adobe Connect envia um email mensal sobre a capacidade de sua conta. Por padrão, os relatórios mensais de capacidade de conta são enviados às 3:00 UTC. Se você quiser que o Adobe Connect envie o email em um horário diferente, adicione parâmetros ao arquivo custom.ini e defina os valores desejados.

1 Abra o arquivo *PastaInstalaçãoRaiz* \custom.ini e adicione os seguintes parâmetros ao arquivo, com os valores desejados:

THRESHOLD_MAIL_TIME_OF_DAY_HOURS A hora UTC em que os relatórios mensais para notificações de capacidade devem ser enviados. Esse valor precisa ser um número inteiro entre 0 e 23. Esse parâmetro pode ser definido somente no arquivo custom.ini, não podendo ser definido no Adobe Connect Central.

THRESHOLD_MAIL_TIME_OF_DAY_MINUTES Os minutos quando os relatórios mensais para notificações de capacidade são enviados. Esse valor precisa ser um número inteiro de 0 a 59. Esse parâmetro pode ser definido somente no arquivo custom.ini, não podendo ser definido no Adobe Connect Central.

Nota: *Se algum dos parâmetros acima não for especificado ou for especificado incorretamente, o email será enviado às 3:00 (UTC).*

Estes são exemplos de valores adicionados ao arquivo custom.ini:

```
THRESHOLD_MAIL_TIME_OF_DAY = 5
THRESHOLD_MAIL_TIME_OF_MINUTES = 30
```

2 Faça o seguinte para reiniciar o Connect:

a Clique em Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Application Server.

b Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Application Server.

Definir limites de capacidade

Os administradores de conta do Connect podem definir limites de capacidade no Adobe Connect Central. Quando a conta ultrapassa esses limites, uma notificação é enviada. É possível adicionar parâmetros ao arquivo custom.ini que definem os limites de capacidade padrão no Adobe Connect Central.

Para obter mais informações sobre a configuração de notificações de conta no Adobe Connect Central, consulte o capítulo “Administração do Adobe Connect” em *Uso do Adobe Connect 8*, disponível online em www.adobe.com/br/support/connect.

1 Abra o arquivo *PastaInstalaçãoRaiz*\custom.ini e adicione quaisquer dos seguintes parâmetros ao arquivo, com os valores desejados:

THRESHOLD_NUM_OF_MEMBERS A porcentagem limite padrão para a cota de autores e hosts de reunião. Esse valor precisa ser um número inteiro de 10 a 100, divisível por 10. Se o valor não for especificado ou for especificado incorretamente, o valor será 80.

THRESHOLD_CONC_USERS_PER_MEETING A porcentagem limite padrão para a cota de usuários simultâneos por reunião. Esse valor precisa ser um número inteiro de 10 a 100, divisível por 10. Se o valor não for especificado ou for especificado incorretamente, o valor será 80.

THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT A porcentagem limite padrão da cota de participantes de reuniões em toda a conta. Esse valor precisa ser um número inteiro de 10 a 100, divisível por 10. Se o valor não for especificado ou for especificado incorretamente, o valor será 80.

THRESHOLD_CONC_TRAINING_USERS A porcentagem limite padrão da cota de alunos simultâneos. Esse valor precisa ser um número inteiro de 10 a 100, divisível por 10. Se o valor não for especificado ou for especificado incorretamente, o valor será 80.

Estes são exemplos de valores adicionados ao arquivo custom.ini:

```
THRESHOLD_NUM_OF_MEMBERS = 90
THRESHOLD_CONC_USERS_PER_MEETING = 90
THRESHOLD_CONC_MEETING_USERS_PER_ACCOUNT = 90
THRESHOLD_CONC_TRAINING_USERS = 75
```

2 Faça o seguinte para reiniciar o Connect:

a Clique em Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Application Server.

b Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Application Server.

Configuração do valor de limite de tempo de sessão

As sessões do Adobe Connect incluem o Adobe Connect Meeting e o Connect Central. O limite de tempo de sessão especifica quanto tempo uma sessão poderá ficar ociosa antes de o servidor desconectá-la. Quando uma sessão for desconectada, o usuário será redirecionado para a página de logon do Connect Central.

O valor de limite de tempo do Adobe Connect 8 é de 30 minutos. Os administradores de conta podem alterar esse valor na guia Administração do Connect Central. Os administradores do sistema também podem alterar o valor do limite de tempo de sessão no arquivo custom.ini. O valor no Connect Central tem precedência sobre o valor no arquivo custom.ini.

Para configurar o limite de tempo de sessão no arquivo custom.ini:

1 Em um editor de texto, abra *[dir_instalação_raiz]*\custom.ini.

2 Adicione o seguinte parâmetro e o defina como o valor desejado, em segundos:

```
SESSION_TIMEOUT = 3600
```

***Nota:** Esse valor altera o limite de tempo de sessão de 30 para 60 minutos.*

3 Salve o arquivo custom.ini.

4 Reinicie o servidor do aplicativo e o servidor de reunião.

Importante: *Antes do Adobe Connect 8, o limite de tempo de sessão era de 16 horas. Talvez você precise atualizar aplicativos que usem a API do Adobe Connect Web Services para captar um limite de tempo de sessão e realizar novamente a autenticação.*

Mais tópicos da Ajuda

"Iniciar e parar os servidores" na página 81

Configuração de conversão de PDF em SWF

Sobre a conversão de PDF

Você pode usar o pod de compartilhamento em uma sala de reuniões do Adobe Connect para compartilhar documentos PDF. Os hosts e os apresentadores podem sincronizar a navegação para todos os participantes e usar o quadro branco sobreposto para colaborar. Você pode carregar documentos PDF no pod de compartilhamento pela área de trabalho ou pela biblioteca de conteúdo do Adobe Connect. Compartilhar documentos no pod de compartilhamento oferece as seguintes vantagens sobre o compartilhamento de telas:

- Os hosts e os apresentadores podem organizar e carregar antecipadamente os documentos na sala de reuniões.
- Qualidade superior de exibição para todos os participantes.
- Requisitos de largura de banda inferiores para participantes e apresentadores.
- Mais fácil para vários apresentadores trabalharem juntos.
- Mais fácil para colaborar usando o quadro branco.

Quando os documentos PDF forem compartilhados em um pod de compartilhamento, o Adobe Connect os converterá no formato Flash. O Adobe Connect Server oferece parâmetros de configuração para controlar a conversão de PDF.

Configurar a conversão de PDF em SWF

1 Abra o arquivo *PastadaInstalaçãoRaiz*\custom.ini em um editor de texto.

2 Edite um dos seguintes parâmetros de configuração:

Parâmetro	Valor padrão	Descrição
`ENABLE_PDF2SWF`	true	Um valor booleano que especifica se a conversão de PDF em SWF está ativada ou não para o servidor. Defina esse parâmetro como falso para desativar a conversão devido a problemas de desempenho.
`PDF2SWF_PAGE_TIMEOUT`	5	O valor do tempo limite por página, em segundos.
`PDF2SWF_CONVERTER_PORTS_START`	4000	O valor mais baixo do intervalo de portas usado para conversões de PDF em SWF.
`PDF2SWF_CONVERTER_PORTS_END`	4030	O valor mais alto do intervalo de portas usado para conversões de PDF em SWF.

Parâmetro	Valor padrão	Descrição
PDF2SWF_CONCURRENCY_LIMIT	3	O número máximo de conversões simultâneas de PDF em SWF que podem ser executadas em um servidor de aplicativos. Se um servidor de aplicativos receber mais solicitações, elas serão enfileiradas.
PDF2SWF_QUEUE_LIMIT	5	O número máximo de conversões de PDF em SWF que podem aguardar em uma fila por vez. Se um servidor de aplicativos receber mais solicitações, um usuário receberá a mensagem "O Adobe Connect não pôde converter o arquivo para exibição. Tente novamente mais tarde". ". Um administrador vê o seguinte nos registros: <status code="request-retry"><exception>java.lang.Exception: Conversion Load too much on server.
PDF2SWF_TIMEOUT_NUMBER_OF_PAGES	3	O número máximo de páginas com tempo limite permitido antes de a conversão ser parada.

3 Reinicie o Adobe Connect Central Application Server. Consulte "Iniciar e parar o Adobe Connect" na página 81.

Integração com o Microsoft Live Communications Server 2005 e Microsoft Office Communications Server 2007

Fluxo de trabalho para configuração da integração de presença

Integre o Connect a um servidor de comunicações em tempo real da Microsoft para que os hosts de reunião possam ver a presença LCS ou OCS dos participantes da reunião registrados na lista de convidados e iniciar conversas baseadas em texto com usuários online.

1. O Connect Server e um servidor de comunicações precisam ser instalados.

Instale e verifique a instalação do Connect Server e de um servidor de comunicações. O Connect Server oferece suporte à integração com o Microsoft Live Communications Server 2005 e Microsoft Office Communications Server 2007. Consulte "Instalar o Adobe Connect 8" na página 20 e a documentação do servidor de comunicação.

2. Configure o servidor de comunicações.

Configure o servidor de comunicações de forma que troque dados com o Adobe Connect. Consulte "Configurar o Live Communications Server 2005" na página 60ou "Configurar o Office Communications Server 2007" na página 61.

3. Pare o Adobe Connect Presence Service.

O Adobe Connect Server inclui o Adobe Connect Presence Service. Pare o serviço antes de configurar o Connect. Consulte "Iniciar e parar o Adobe Connect Presence Service" na página 65.

4. Configure o Adobe Connect Presence Service.

Configure o Adobe Connect para que troque dados com o servidor de comunicações. O servidor de presença está instalado em *PastadaInstalaçãoRaiz*\presserv. Consulte "Configuração do Adobe Connect Presence Service" na página 62.

5. Inicie o Adobe Connect Presence Service.

Consulte “Iniciar e parar o Adobe Connect Presence Service” na página 65.

6. Ative a lista de convidados e o pod de bate-papo no Adobe Connect Central.

Faça logon no Adobe Connect Central como administrador. Selecione Administração > Conformidade e controle > Gerenciamento de pods. Desmarque a opção para ativar a lista de convidados e o pod de bate-papo.

Configurar o Live Communications Server 2005

***Nota:** Se você estiver instalando o Office Communications Server 2007, consulte “Configurar o Office Communications Server 2007” na página 61.*

1 Escolha Iniciar > Programas > Ferramentas administrativas > Live Communications Server 2005 para abrir o console de configuração.

2 Clique com o botão direito do mouse na floresta, selecione Propriedades e execute este procedimento:

a Selecione a guia Federação.

b Selecione a caixa de seleção Ativar federação e conectividade para mensagens instantâneas públicas.

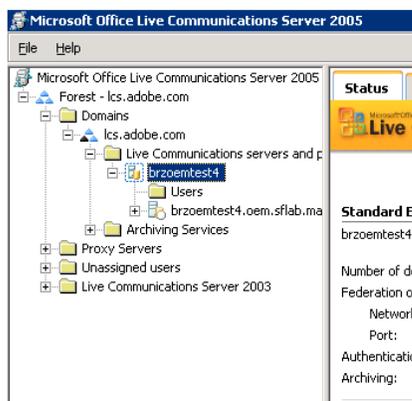
c Insira o endereço de rede do Connect

d Insira a porta 5072.

5072 é o número da porta padrão do Adobe Connect Presence Service no arquivo \presserv\conf\lcsgw.xml.

e Clique em OK.

3 No painel esquerdo do console de configuração, expanda Domínios, expanda o seu domínio e expanda servidores e pools do Live Communications.

4 Clique com o botão direito do mouse no nome de host de seu pool e selecione Propriedades.

5 Na caixa de diálogo Propriedades do servidor, execute este procedimento:

a Selecione a guia Autorização do host. Adicione o endereço IP do Connect. Certifique-se de que Somente de saída esteja definido como Não, Restringir como servidor, como Sim e Tratar como autenticação, como Sim.

b Se houver um balanceador de carga instalado à frente do servidor Connect , adicione o endereço IP do balanceador de carga.

c Clique em OK.

6 No painel esquerdo do console de configuração, expanda o FQDN do servidor e selecione Aplicativos.

7 Execute este procedimento:

a Clique em IM URL Filter Application Setting. Na caixa de diálogo Propriedades, desmarque Habilitar. Se essa configuração estiver ativada, os hosts de reunião não poderão enviar URLs em mensagens instantâneas.

8 Feche o console de configuração.

Configurar o Office Communications Server 2007

***Nota:** Se você estiver instalando o Live Communications Server 2005, consulte "Configurar o Live Communications Server 2005" na página 60.*

1 Escolha Iniciar > Programas > Ferramentas administrativas > Office Communications Server 2007 para abrir o console de configuração.

2 Clique com o botão direito do mouse na Floresta, selecione Propriedades e então selecione Propriedades globais.

3 Selecione a guia Geral, adicione ou selecione um domínio padrão e então clique em OK.

4 Selecione a guia Federação e faça o seguinte:

a Selecione a caixa de seleção Ativar federação e conectividade para mensagens instantâneas públicas.

b Insira o FQDN do Office Communications Server 2007.

c Insira a porta 5072.

5072 é o número da porta padrão do Adobe Connect Presence Service no arquivo \presserv\conf\lcsgw.xml.

d Clique em OK.

5 Na Floresta, clique com o botão direito do mouse no nome do host, selecione Propriedades e então selecione Propriedades de front-end.

6 Selecione a guia Autenticação, escolha NTLM como o protocolo de autenticação e clique em OK.

7 Selecione a guia Autorização de host e faça o seguinte:

a Adicione o endereço IP do sistema Adobe Connect.

b Select as caixas de seleção Restringir como Servidor e Tratar como Autenticado.

c Clique em OK.

8 Clique com o botão direito do mouse no nome de host e nome de domínio (por exemplo, brzoemtest5.oem.sflab.macromedia.com) e selecione Propriedades > Propriedades do front-end.

9 Selecione a guia Geral e faça o seguinte:

a Adicione a porta 5072, Transporte TCP, Endereço Todos.

b Adicione a porta 5060, Transporte MTLS, Endereço Todos.

c Adicione a porta 5061, Transporte MTLS, Endereço Todos.

d Habilite todas as três portas e clique em OK.

10 Selecione a guia Conferência de IM e faça o seguinte:

a Defina o endereço IP como o endereço do OCS 2007 Server.

b Defina a porta de escuta SIP como 5062.

c Clique em OK.

11 Selecione a guia Conferência de telefonia e faça o seguinte:

a Defina o endereço IP como o endereço do OCS 2007 Server.

b Defina a porta de escuta SIP como 5064.

c Clique em OK.

12 Selecione a guia Certificado.

Você verá as informações sobre seu certificado SSL.

13 Na Floresta, expanda o nome de host e o nome de domínio (por exemplo, brzoemtest5.oem.sflab.macromedia.com) e faça o seguinte:

a Clique com o botão direito do mouse em Aplicativos e selecione Propriedades.

b Certifique-se de que a opção Intelligent IM URL Filter Application Setting (Configuração de aplicativo de filtro de URL de IM inteligente) não esteja habilitada e clique em OK.

14 Feche o console de configuração.

15 Se você estiver atualizando do Live Communications Server 2005, realize as etapas a seguir para cada usuário, a fim de habilitar a presença aperfeiçoada:

a Selecione Iniciar > Programas > Ferramentas administrativas > Usuários e computadores do Active Directory.

b Clique com o botão direito no nome do usuário e selecione Habilitar usuários para Servidor de Comunicações.

Configurar clientes do servidor de comunicações

A integração do Connect com os servidores de comunicações da Microsoft funciona com clientes padrão do Microsoft Office Communicator 2005 (MOC 2005). Os clientes não requerem nenhuma configuração especial. No entanto, para tornar os URLs nas reuniões do Connect clicáveis no MOC 2005, modifique a propriedade “Permitir hiperlinks em mensagens instantâneas” do modelo administrativo do Communicator. Para obter mais informações, consulte http://technet.microsoft.com/pt-br/library/bb963959(en-us).aspx.

1 Escolha Iniciar > Executar.

2 Insira gpedit.msc na caixa Abrir para abrir a janela Diretiva de grupo.

3 Clique para expandir Configuração do computador.

4 Clique para expandir Modelos administrativos.

5 Clique com o botão direito do mouse em Configurações de política do Communicator e escolha Propriedades.

Nota: *Se o modelo Configurações de política do Microsoft Office Communicator não estiver presente na pasta Modelos administrativos, adicione-o. Localize o arquivo Communicator.adm no pacote de cliente do Microsoft Office Communicator 2005 e copie-o em C:\WINDOWS\inf\. Na janela Diretiva de grupo, clique com o botão direito do mouse em Modelos administrativos, clique em Adicionar/remover modelos, clique em Adicionar, navegue até o arquivo e clique em Abrir.*

Configuração do Adobe Connect Presence Service

Conclua os quatro procedimentos a seguir para configurar o Adobe Connect Presence Service de forma a trocar dados com um servidor de comunicações. Depois de concluir a configuração, reinicie o Adobe Connect Central Application Server.

Definir a conexão de gateway entre o Adobe Connect Presence Service e o servidor de comunicações

1 Abra o arquivo *PastadaInstalaçãoRaiz*\presserv\conf\lcsgw.xml em um editor de XML.

2 Edite o arquivo para que fique como segue, substituindo os valores em negrito por seus próprios valores:

```
<?xml version="1.0" encoding="UTF-8"?>
<config>
<block xmlns="accept:config:sip-lcsgw">
<service trace="off" name="lcsgw" id="internal.server">
<stack name="lcs">
<via/>
</stack>
<state type="enabled"/>
<host type="external">lcs.adobe.com</host>
<domain-validation state="false"/>
<binding name="connector-0" transport="tcp">
<port>5072</port>
<bind>10.59.72.86</bind> <!-- LCS server IP -->
<area>lcs.adobe.com</area> <!-- LCS domain -->
</binding>
</service>
</block>
</config>
```

Parâmetro	Descrição
`<host>`	O território SIP de usuários LCS ou OCS.
`<bind>`	Endereço IP do servidor LCS ou OCS (ou do balanceador de carga)
`<area>`	O território SIP de usuários LCS ou OCS.

Configurar o arquivo custom.ini

1 Abra o arquivo *PastadaInstalaçãoRaiz*\custom.ini em um editor de texto.

2 Insira os seguintes parâmetros e valores:

Parâmetro	Valor
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Este valor distingue maiúsculas de minúsculas.
OPN_HOST	O endereço de rede do Adobe Connect Presence Service (por exemplo, localhost).
OPN_PORT	A porta interna usada entre o Connect e o Adobe Connect Presence Service. O valor padrão (10020) deve corresponder ao valor no arquivo *PastadaInstalaçãoRaiz*\presserv\conf\router.xml Não modifique esse valor.
OPN_PASSWORD	O token interno usado entre o Connect e o Adobe Connect Presence Service. O valor padrão (secret) deve corresponder ao valor no arquivo *PastadaInstalaçãoRaiz*\presserv\conf\router.xml. Não modifique esse valor.
OPN_DOMAIN	O nome do domínio do Connect Server (servidor de aplicativos). O Adobe Connect Presence Service usa esse nome para identificar o servidor de aplicativos. Em um cluster, cada servidor de aplicativos precisa ter seu próprio nome de domínio.
MEETING_PRESENCE_POLL_INTERVAL	Os clientes de host sondam o servidor de presença periodicamente para recuperar o status dos convidados. Esse parâmetro define o número de segundos entre as solicitações de sondagem. O valor padrão é 30. Não modifique esse valor.

Veja a seguir exemplos de configurações:

```
OPN_ADAPTOR=com.macromedia.breeze.opn.OPNGateway
OPN_HOST=localhost
OPN_PORT=10020
OPN_PASSWORD=secret
OPN_DOMAIN=breeze01.com
```

Definição do gateway SIP para o Adobe Connect Presence Service

1 Abra o arquivo *PastadaInstalaçãoRaiz*\presserv\conf\router.xml em um editor de XML.

2 Edite o arquivo para que fique como segue, substituindo os valores em negrito por seus próprios valores:

```
<block xmlns="accept:config:xmpp-gateway">
...
<block xmlns="accept:config:sip-stack-manager">
<service trace="off">
<bind>10.133.192.75</bind> <!-- presence server machine IP -->
<state type="enabled"/></service></block>
```

Na tag `<bind>`, insira o endereço IP do computador que hospeda o Connect. Se vários endereços IP forem retornados, selecione o endereço IP interno ou externo que o servidor remoto LCS ou OCS possa resolver para a conexão com o Connect.

3 Reinicie o Adobe Connect Central Application Server.

Configuração do Adobe Connect Presence Service em um cluster

Se você estiver executando o Adobe Connect em um cluster, execute o Adobe Connect Presence Service somente em um computador no cluster. Contudo, configure o Adobe Connect Presence Service em todos os computadores no cluster para que eles possam trocar tráfego de presença.

1 Abra o arquivo *[DiretóriodaInstalaçãoRaiz]*\custom.ini em um editor de texto.

2 Insira os seguintes parâmetros e valores:

Parâmetro	Valor
OPN_ADAPTOR	com.macromedia.breeze.opn.OPNGateway Este valor distingue maiúsculas de minúsculas.
OPN_HOST	O FQDN do computador que executa o Adobe Connect Presence Service. O valor do parâmetro OPN_HOST é o mesmo em todos os computadores no cluster.
OPN_PORT	A porta interna usada entre o Connect e o Adobe Connect Presence Service. O valor padrão (10020) deve corresponder ao valor no arquivo *PastadaInstalaçãoRaiz*\presserv\conf\router.xml Não modifique esse valor.
OPN_PASSWORD	O token interno usado entre o Connect e o Adobe Connect Presence Service. O valor padrão (secret) deve corresponder ao valor no arquivo *PastadaInstalaçãoRaiz*\presserv\conf\router.xml. Não modifique esse valor.
OPN_DOMAIN	O domínio Adobe Connect Presence Service usa para identificar um servidor Adobe Connect em um cluster. Cada computador em um cluster tem um valor exclusivo. O parâmetro OPN_DOMAIN pode ter qualquer valor (por exemplo, presence.connect1, presence.connect2, connect3) desde que o valor seja exclusivo dentro do cluster.
MEETING_PRESENCE_POLL_INTERVAL	Os clientes de host sondam o servidor de presença periodicamente para recuperar o status dos convidados. Esse parâmetro define o número de segundos entre as solicitações de sondagem. O valor padrão é 30. Não modifique esse valor.

Veja a seguir exemplos de configurações:

```
OPN_ADAPTOR=com.macromedia.breeze.opn.OPNGateway
OPN_HOST=localhost
OPN_PORT=10020
OPN_PASSWORD=secret
OPN_DOMAIN=presence.connect1
```

3 Reinicie o Adobe Connect Central Application Server.

Iniciar e parar o Adobe Connect Presence Service

É possível iniciar e parar o Adobe Connect Presence Service no menu Iniciar ou na janela Serviços.

Iniciar e parar o Adobe Connect Presence Service no menu Iniciar

❖ Execute um dos procedimentos a seguir:

- Escolha Iniciar > Programas > Adobe Adobe Connect Server > Iniciar o Connect Presence Service.
- Escolha Iniciar > Programas > Adobe Connect Server > Parar o Connect Presence Service.

Iniciar e parar o Adobe Connect Presence Service na janela Serviços

1 Para abrir a janela Serviços, clique em Iniciar > Painel de controle > Ferramentas administrativas > Serviços.

2 Selecione Connect Presence Service e clique em Iniciar o serviço, Parar o serviço ou Reiniciar o serviço.

Configuração de logon único (SSO)

Sobre o logon único

O logon único é um mecanismo que permite que um usuário se autentique uma vez e obtenha acesso a vários aplicativos. O logon único usa um servidor proxy para autenticar os usuários, de forma que eles não precisem fazer logon no Connect.

O Connect oferece suporte aos seguintes mecanismos de logon único:

Autenticação do cabeçalho HTTP Configurar um proxy de autenticação para interceptar a solicitação HTTP, analisar as credenciais do usuário no cabeçalho e passá-las para o Connect.

Autenticação do Microsoft NT LAN Manager (NTLM) Configure o Adobe Connect para tentar conectar automaticamente clientes autenticados em um controlador de domínio do Windows, usando o protocolo NTLMv1. O Microsoft Internet Explorer no Microsoft Windows pode negociar autenticação NTLM sem pedir as credenciais do usuário.

Nota: *A autenticação NTLM não funciona em servidores de borda. Use o método de autenticação LDAP.*

Nota: *Os clientes Mozilla Firefox podem negociar uma autenticação NTLM sem solicitação. Para obter informações sobre configuração, consulte este documento do Firefox.*

Você também pode escrever seu próprio filtro de autenticação. Para obter mais informações, entre em contato com o Suporte da Adobe.

Configurar a autenticação do cabeçalho HTTP

Quando a autenticação do cabeçalho HTTP é configurada, as solicitações de logon do Connect são encaminhadas a um agente posicionado entre o cliente e o Connect. O agente pode ser um proxy de autenticação ou um software que autentique o usuário, adicione outro cabeçalho à solicitação HTTP e a envie ao Connect. No Connect , você deve excluir as barras de comentário do filtro de Java e configurar um parâmetro no arquivo custom.ini, que especifica o nome do cabeçalho HTTP adicional.

Mais tópicos da Ajuda

"Iniciar e parar o Adobe Connect" na página 81

Configurar a autenticação de cabeçalho HTTP no Adobe Connect

Para habilitar a autenticação do cabeçalho HTTP, configure um mapeamento do filtro Java e um parâmetro de cabeçalho no computador que hospeda o Connect.

1 Abra o arquivo *[dir_instalação_raiz]*\appserv\web\WEB-INF\web.xml e execute este procedimento:

a Remova as marcas de comentário em torno dos elementos de mapeamento de filtro e filtro para HeaderAuthenticationFilter.

b Adicione marcas de comentário em torno do filtro filtroNtlmAuthenticationFilter e elementos de mapeamento de filtro.

2 Pare o Connect:

a Clique em Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Application Server.

b Clique em Iniciar > Programas > Adobe Connect Server > Parar o Connect Meeting Server.

3 Adicione a linha a seguir ao arquivo custom.ini:

```
HTTP_AUTH_HEADER=header_field_name
```

Seu agente de autenticação deverá adicionar uma solicitação HTTP, que será enviada ao Connect. O nome do cabeçalho deverá ser `header_field_name`.

4 Salve o arquivo custom.ini e reinicie o Connect:

a Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Meeting Server.

b Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Application Server.

Escrever o código de autenticação

O código de autenticação deve autenticar o usuário, adicionar um campo ao cabeçalho HTTP que contiver o logon do usuário e enviar uma solicitação ao Connect.

1 Defina o valor do campo de cabeçalho `header_field_name` como um logon de usuário do Connect

2 Envie uma solicitação HTTP ao Connect no seguinte URL:

```
http://connectURL/system/login
```

O filtro Java do Connect pega a solicitação, procura pelo cabeçalho `header_field_name` e procura por um usuário com a ID transmitida no cabeçalho. Se o usuário for localizado, ele será autenticado e será enviada uma resposta.

3 Analise o conteúdo HTTP da resposta do Connect para obter a string `"OK"` , indicando uma autenticação bem-sucedida.

4 Analise a resposta do Connect para obter o cookie `BREEZESESSION`.

5 Redirecione o usuário para o URL requisitado no Connect e passe o cookie `BREEZESESSION` como valor do parâmetro `session`, da seguinte forma:

```
http://connectURL?session=BREEZESESSION
```

Nota: *Você deve passar o cookie* `BREEZESESSION` *em todas as solicitações posteriores do Connect durante esta sessão do cliente.*

Configurar a autenticação do cabeçalho HTTP com o Apache

O procedimento a seguir descreve um exemplo da implementação da autenticação do cabeçalho HTTP que usa o Apache como agente de autenticação.

1 Instale o Apache como proxy reverso em um computador diferente daquele que armazena o Connect.

2 Escolha Iniciar > Programas > Apache HTTP Server > Configure Apache Server > Edit the Apache httpd.conf (arquivo de configuração) e execute este procedimento:

a Exclua as barras de comentário da seguinte linha:

```
LoadModule headers_module modules/mod_headers.so
```

b Exclua as barras de comentário das três linhas a seguir:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

c Adicione as linhas a seguir ao final do arquivo:

```
RequestHeader append custom-auth "ext-login"
ProxyRequests Off
<Proxy *>
Order deny,allow
Allow from all
</Proxy>
ProxyPass / http://hostname:[port]/
ProxyPassReverse / http://hostname:[port]/
ProxyPreserveHost On
```

3 Pare o Connect:

a Clique em Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Application Server.

b Clique em Iniciar > Programas > Adobe Connect Server > Parar o Connect Meeting Server.

4 No computador que estiver hospedando o Connect , adicione as seguintes linhas de código ao arquivo custom.ini (localizado no diretório raiz de instalação, c:\breeze, por padrão):

```
HTTP_AUTH_HEADER=custom-auth
```

O parâmetro `HTTP_AUTH_HEADER` deve corresponder ao nome configurado no proxy (neste exemplo, ele foi configurado na linha 1 da etapa 2c). O parâmetro é o cabeçalho HTTP adicional.

5 Salve o arquivo custom.ini e reinicie o Connect:

a Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Meeting Server.

b Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Application Server.

6 Abra o arquivo *[dir_instalação_raiz]*\appserv\web\WEB-INF\web.xml e execute este procedimento:

a Cancele o comentário do filtro HeaderAuthenticationFilter completo.

b Comente o filtro NtlmAuthenticationFilter completo.

Configurar autenticação NTLM

O NTLMv1 é um protocolo de autenticação usado com o protocolo de rede SMB nas redes do Microsoft Windows. Você pode usar o NTLM para permitir que um usuário forneça sua identidade para um domínio do Windows uma vez e posteriormente para ser autorizado a acessar outro recurso de rede, como o Adobe Connect. Para estabelecer as credenciais de usuário, o navegador da Web do usuário gera automaticamente uma contestação e uma resposta de autenticação com o controlador de domínio através do Adobe Connect. Se esse mecanismo falhar, o usuário poderá fazer logon diretamente no Adobe Connect Somente o Internet Explorer no Windows oferece suporte a single sign-on com autenticação NTLMv1.

Nota: *Por padrão, os controladores de domínio do Windows Server 2003 exigem um recurso de segurança chamado assinaturas SMB. As assinaturas SMB não são compatíveis com a configuração padrão do filtro de autenticação NTLM. Você pode configurar o filtro para funcionar com esse requisito. Para obter mais informações sobre isso e outras opções de configuração avançada, consulte a JCIFS NTLM HTTP documentação de autenticação.*

Adicionar parâmetros de configuração

Execute os procedimentos a seguir para cada host de um Adobe Connect:

1 Abra o arquivo *[diretório_instalação_raiz]*\custom.ini no editor de texto e adicione os seguintes parâmetros:

```
NTLM_DOMAIN=[domain]
NTLM_SERVER=[WINS_server_IP_address]
```

O valor `[domain]` é o nome do domínio do Windows dos quais os usuários são membros e nos quais ele são autenticados, por exemplo, CORPNET. Talvez seja necessário definir esse valor para o nome de domínio compatível de uma versão compatível anterior ao Windows 2000. Para obter mais informações, consulte Notá técnica 27e73404. Esse valor é mapeado para a propriedade de filtro `jcifs.smb.client.domain`. Configurar o valor diretamente no arquivo web.xml substitui o valor no arquivo custom.ini.

O valor `[WINS_server_IP_address]` é o endereço IP ou uma lista separada por vírgulas de endereços IP de servidores WINS. Use o endereço IP, o nome de host não funciona. Os servidores WINS são consultados na ordem especificada para resolver o endereço IP de um controlador de domínio especificado no parâmetro `NTLM_DOMAIN`. O controlador de domínio autentica usuários. Você também pode especificar o endereço IP do controlador de domínio, por exemplo, 10.169.10.77, 10.169.10.66. Esse valor é mapeado para a propriedade de filtro `jcifs.netbios.wins`. Configurar o valor no arquivo web.xml substitui o valor no arquivo custom.ini.

2 Salve o arquivo custom.ini.

3 Abra o arquivo *[dir_instalação_raiz]*\appserv\web\WEB-INF\web.xml em um editor de texto e execute o procedimento a seguir:

a Remova as marcas de comentário em torno dos elementos de mapeamento de filtro e NtlmAuthenticationFilter inteiro.

b Adicione marcas de comentário aos elementos de mapeamento de filtro e filtro HeaderAuthenticationFilter.

4 Salve o arquivo web.xml.

5 Reinicie o Adobe Connect.

a Escolha Iniciar > Todos os Programas > Adobe Connect Server > Parar o Adobe Connect Server.

b Escolha Iniciar > Todos os Programas > Adobe Connect Server > Iniciar o Adobe Connect Server.

Reconciliar políticas de logon

O Adobe Connect e o NTLM têm políticas de logon diferentes para a autenticação de usuários. Concilie essas políticas antes de implantar um logon único.

O protocolo NTLM usa um identificador de logon, que pode ser um nome de usuário (jsilva), uma ID de funcionário (1234) ou um nome criptografado, dependendo da política ou da organização. Por padrão, o Adobe Connect usa um endereço de email (jsilva@minhaempresa.com) como identificador do logon. Altere a política de logon do Adobe Connect para que ele compartilhe um identificador exclusivo com NTLM.

1 Abra o Adobe Connect Central.

Para abrir o Adobe Connect Central, abra uma janela do navegador e digite o FQDN do Host do Adobe Connect (por exemplo, http://connect.exemplo.com). Você inseriu o valor do host do Adobe Connect na tela Configurações do servidor do console de Gerenciamento de Aplicativo.

2 Selecione a guia Administração. Clique em Usuários e grupos. Clique em Editar políticas de logon e senha.

3 Na seção Política de logon, selecione Não para Usar o endereço de email como logon.

Configurar um proxy reverso na frente do Adobe Connect

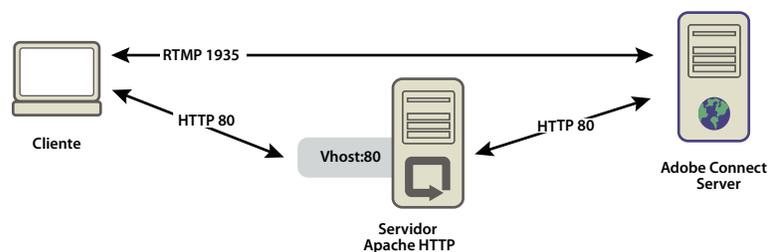
Uso de um proxy reverso

Você pode configurar um proxy reverso na frente do Adobe Connect. O tráfego flui pelo proxy reverso antes de chegar ao Adobe Connect. Use esta configuração para executar o seguinte procedimento:

- Mantenha o Adobe Connect fora do DMZ.

  Coloque o proxy reverso no DMZ e o Adobe Connect atrás do firewall da sua organização.

- Autentique os usuários antes que eles cheguem ao Adobe Connect.

  O proxy reverso autentica os usuários em outro sistema e os autoriza a se conectar ao Adobe Connect.

O tráfego HTTP flui pelo Apache HTTP Server para chegar ao Adobe Connect.

Configurar um proxy reverso

Esse exemplo usa a instalação do Windows (32 bits) do Apache HTTP Server. A configuração é idêntica em qualquer sistema operacional compatível com o Apache. Esse exemplo não usa tráfego SSL; o tráfego para o servidor de aplicativos do Adobe Connect não é criptografado.

Nota: *Quando você atualizar o Adobe Connect, libere o cache de proxy para garantir que novas versões de arquivo sejam atendidas.*

Execute os procedimentos a seguir para forçar todo o tráfego HTTP a passar pelo Apache HTTP Server antes de chegar ao Adobe Connect:

Nota: *O tráfego RTMP não passa pelo Apache HTTP Server nesta configuração.*

1 Instale o Apache HTTP Server.

Por padrão, os arquivos de configuração do Apache estão localizados na pasta C:\Arquivos de Programas\Apache Software Foundation\Apache2.2\conf\.

2 Configure o Apache para escutar todo o tráfego na porta 80.

Abra o arquivo C:\Arquivos de Programas\Apache Software Foundation\Apache2.2\conf\httpd.conf em um editor de texto e adicione o seguinte:

```
#
# Listen: Allows you to bind Apache to specific IP addresses and
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
#
#
```

3 Carregue os módulos necessários para operações como um proxy reverso.

No mesmo arquivo (httpd.conf), exclua o comentário nas seguintes linhas:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
```

4 Vincule o arquivo httpd.conf ao arquivo de configuração que direciona conexões para o Adobe Connect.

Adicione a seguinte linha como a última linha no arquivo httpd.conf:

```
Include conf/extra/httpd-connect.conf
```

5 Crie um arquivo de texto chamado httpd-connect.conf e salve-o em C:\Arquivos de Programas\Apache Software Foundation\Apache2.2\conf\extra.

6 Adicione as seguintes linhas ao arquivo httpd-connect.conf (insira seus endereços IP e portas onde solicitado):

```
#vhost for application server
<VirtualHost *:80>
ProxyRequests Off
ProxyPreserveHost On
ProxyPass / http://<IP-of-Connect-Application-Server>:80/
ProxyPassReverse / http://<IP-of-Connect-Application-Server>:80/
ServerName <FQDN of Apache host>
</VirtualHost>
```

7 Salve o arquivo e reinicie o serviço Apache.

8 Abra o Console de Gerenciamento de Aplicativos do Adobe Connect em um navegador: http://localhost:8510/console/

9 Na tela Configurações do servidor, execute os procedimentos a seguir:

- Defina o host do Adobe Connect no FQDN do Apache HTTP Server.
- Defina o Nome externo para o FQDN do computador que hospeda o Connect Meeting Server.

10 Reinicie o Adobe Connect Service (o servidor de aplicativos) e o serviço Flash Media Server (FMS) (o servidor de reuniões). Consulte “Iniciar e parar os servidores” na página 81.

O RTMP é roteado para o Adobe Connect e o HTTP é roteado pelo Apache.

Hospedagem do Adobe Connect Add-in

Sobre o Adobe Connect Add-in

O Adobe Connect Add-in é uma versão do Flash Player que inclui recursos avançados do Adobe Connect.

Quando o Adobe Connect Add-in for solicitado, o respectivo download será feito de um servidor da Adobe em um processo integrado que não é visto pelo usuário. No entanto, caso sua organização não permita que os funcionários baixem softwares de servidores externos, você poderá armazenar o Adobe Connect Add-in em seu próprio servidor.

Os convidados, os usuários registrados e os apresentadores da reunião serão solicitados a baixar o Connect Add-in caso eles tenham uma versão antiga instalada e sejam promovidos a host ou apresentador, ou ainda recebam direitos avançados ao pod de compartilhamento.

Os hosts e apresentadores da reunião precisam baixar o Connect Add-in caso ele não esteja instalado ou se uma versão antiga estiver instalada.

Personalizar o local de download do Connect Add-in

Você pode hospedar o Connect Add-in no seu servidor e enviar os usuários diretamente para os arquivos executáveis. É possível enviar os usuários a uma página com instruções de download que contém links para os arquivos executáveis. Você pode criar sua própria página de instruções de download ou usar a fornecida pela Adobe. A página da Adobe está traduzida para todos os idiomas suportados.

Enviar os usuários diretamente para os arquivos executáveis:

1 Localize os arquivos XML de idioma do Adobe Connect no servidor que estiver hospedando o Adobe Connect. Os arquivos XML estão nos dois diretórios a seguir:*[dir_instalação_raiz]*\appserv\common\intro\lang e *[dir_instalação_raiz]*\appserv\common\meeting\lang.

2 Em cada arquivo de idioma, insira um caminho para os arquivos executáveis para cada plataforma:

```
<m id="addInLocation" platform="Mac OSX">/common/addin/ConnectAddin.z</m>
<m id="addInLocation" platform="Windows">/common/addin/setup.exe</m>
<m id="addInLocation" platform="Linux">/common/addin/ConnectAddin.deb</m>
```

Nota: *Esses são os locais padrão dos arquivos executáveis do add-in. Você pode alterar os locais no seu servidor e atualizar o caminho na seção* `addInLocation`*.*

Enviar os usuários para as páginas de instruções de download fornecidas pela Adobe:

1 Localize os arquivos XML de idioma do Connect no servidor que estiver hospedando o Adobe Connect. Os arquivos XML estão nos dois diretórios a seguir:*[dir_instalação_raiz]*\appserv\common\intro\lang e *[dir_instalação_raiz]*\appserv\common\meeting\lang.

2 Em cada arquivo de idioma, insira o caminho para a página de instruções de download:

```
<m id="addInLocation" platform="Mac OSX">/common/help/#lang#/support/addindownload.htm</m>
<m id="addInLocation" platform="Windows">/common/help/#lang#/support/addindownload.htm</m>
<m id="addInLocation" platform="Linux">/common/help/#lang#/support/addindownload.htm</m>
```

Nota: *O caminho inclui a string* `#lang#`*, que o Adobe Connect traduz para o idioma da reunião no tempo de execução.*

3 Os arquivos addindownload.htm incluem links para os arquivos executáveis do add-in em seus locais padrão no Connect (/common/addin/setup.exe, /common/addin/AdobeConnectAddin.z e /common/addin/ConnectAddin.deb). Se você alterar o local dos arquivos executáveis, atualize os links da página addindownload.htm de cada idioma.

Enviar os usuários para as páginas de instruções de download que você criar:

1 Localize os arquivos XML de idioma do Connect no servidor que estiver hospedando o Connect. Os arquivos XML estão nos dois diretórios a seguir:*[dir_instalação_raiz]*\appserv\common\intro\lang e *[dir_instalação_raiz]*\appserv\common\meeting\lang.

2 Em cada arquivo de idioma, adicione os seguintes caminhos para a página de instruções que você criou:

```
<m id="addInLocation" platform="Mac
OSX">common/help/#lang#/support/addin_install_instructions.html</m>
<m id="addInLocation"
platform="Windows">common/help/#lang#/support/addin_install_instructions.html</m>
<m id="addInLocation"
platform="Linux">common/help/#lang#/support/addin_install_instructions.html</m>
```

Nota: *É possível criar páginas de instrução separadas para cada plataforma.*

3 Crie uma página de instruções em cada idioma que você deseja oferecer suporte. Inclua links na página de instrução para os arquivos executáveis do add-in de cada plataforma.

Capítulo 4: Segurança

A proteção do Adobe® Connect™ protege sua organização contra a perda de dados e atos maliciosos. É importante proteger a infra-estrutura da sua organização, do Adobe Connect e do servidor de banco de dados usado pelo Acrobat Connect.

SSL (secure sockets layer)

Sobre o suporte ao SSL

O Adobe Connect Server consiste em dois servidores: o Adobe® Flash® Media Server e o servidor de aplicativos Acrobat Connect O Flash Media Server é chamado *servidor de reunião* porque proporciona reuniões utilizando uma conexão RTMP em tempo real com o cliente. O servidor de aplicativos Adobe Connect lida com a conexão HTTP entre o cliente e a lógica de aplicativo do Adobe Connect. O Adobe Connect Server também conecta-se a um banco de dados SQL Server.

Nota: *No menu Iniciar, o servidor de reunião é denominado "Connect Meeting Server" e o servidor de aplicativos é denominado "Connect Central Application Server". Na janela Serviços, o servidor de reunião é denominado "Flash Media Server (FMS)" e o servidor de aplicativos é denominado "Adobe Connect Service".*

Você pode configurar o SSL para o servidor de aplicativos, para o servidor de reunião e para o banco de dados.

Solução baseada em hardware Use um acelerador SSL para obter a configuração mais robusta do SSL.

Solução baseada em software Use o suporte nativo a SSL no Adobe Connect.

Nota: *O SSL não é compatível com o Microsoft® Windows® 98.*

O Connect usa o método `CONNECT` do HTTP para solicitar uma conexão SSL. Servidores proxy precisam permitir que os clientes usem o método `CONNECT`. Se os clientes não puderem usar o método `CONNECT`, as conexões RTMP serão encapsuladas por HTTP/HTTPS.

Para obter mais informações sobre como configurar SSL, consulte Configurar SSL para o Adobe Connect Server 8.

Para obter ajuda sobre como configurar SSL, entre em contato com o Suporte da Adobe no site www.adobe.com/support/programs/connect.

PKI (infra-estrutura de chave pública)

Sobre a PKI (infra-estrutura de chave pública)

Você pode definir uma infra-estrutura de chave pública (PKI) para gerenciar credenciais de identificação como parte da sua arquitetura de segurança do Adobe Connect para clientes. No protocolo SSL, que é bastante conhecido, o servidor deve verificar sua identidade com o cliente; em PKI, o cliente deve verificar sua identidade com o servidor.

Uma empresa confiável, chamada de autoridade de certificação, verifica a identidade do cliente e vincula um certificado a esse cliente. O certificado (também denominado *chave pública*) está no formato X.509. Quando o cliente se conecta ao Adobe Connect, um proxy negocia a conexão para a PKI. Se o cliente tiver um cookie de uma sessão anterior ou um certificado válido, ele será conectado ao Adobe Connect.

Para obter mais informações sobre PKI, consulte o Microsoft PKI Technology Center.

Requisitos do usuário de PKI

Os usuários devem executar Windows XP ou Windows 2003 e possuir um certificado do cliente válido instalado no computador local antes de entrar em uma reunião que exija autenticação PKI. Ao entrar em uma reunião, o usuário verá uma caixa de diálogo para selecionar um certificado do cliente válido entre os certificados instalados no computador.

A Adobe recomenda que os clientes usem o Adobe Connect Add-in para participar de reuniões que exijam autenticações PKI. Os clientes precisam usar o instalador independente do add-in para instalá-lo antes de entrar na reunião.

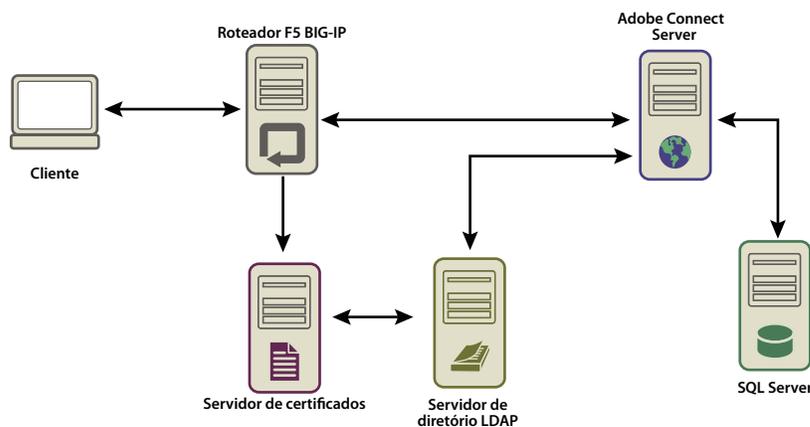
Os clientes também podem usar a última versão do Adobe Flash Player no navegador para entrar nas reuniões, mas o suporte a PKI do Flash Player não é tão extenso quanto o suporte a PKI do add-in. Uma exceção é a de que, para os arquivos mortos da reunião, os clientes devem contar com a versão mais recente do Flash Player.

Você pode desenhar um sistema de PKI para exibir autenticação somente para conexões HTTP ou para conexões HTTP e RTMP. Se você exigir certificados do cliente nas conexões HTTP e RTMP, os usuários serão avisados cada vez que for estabelecida uma nova conexão no servidor. Por exemplo, haverá dois prompts para fazer logon em uma reunião: um para HTTP e outro para RTMP. Como a conexão RTMP não pode ser estabelecida sem a autenticação HTTP, você pode escolher exigir a autenticação do cliente somente na conexão HTTP.

Implementação de PKI

As etapas a seguir o guiarão pela implementação de referência de PKI configurado com o roteador F5 BIG-IP LTM 9.1.2 (Build 40.2) como proxy. Use as seções mais importantes para criar sua própria solução, seja com um roteador F5 ou com outro dispositivo.

Essa implementação de referência obedece a rígidos padrões de segurança. Por exemplo, ela exige um certificado do cliente para as conexões de HTTP (servidor de aplicativos) e para RTMP (servidor de reunião).

Nota: *A Adobe recomenda enfaticamente que você crie uma política de segurança antes de implementar a PKI. Existem várias tecnologias diferentes utilizadas em PKI, e a sustentação da segurança é essencial quando esses sistemas interagem.*

Fluxo de dados em uma infra-estrutura de chave pública

Este exemplo pressupõe o seguinte:

- O Adobe Connect está instalado.

- O Adobe Connect é integrado a um serviço de diretório LDAP.
- Um usuário importado do serviço de diretório LDAP pode entrar em uma reunião hospedada pelo Adobe Connect.
- O roteador F5 está instalado.

1. Configure o servidor do diretório LDAP.

Deve ser especificado um atributo `email` do LDAP para cada usuário. Esse atributo é adicionado ao campo de assunto do certificado do cliente.

O F5 iRule analisa o elemento X.509::subject para obter o endereço de email e insere o valor no cabeçalho HTTP. O Connect usa o cabeçalho HTTP para autenticar o usuário.

Nota: *Este exemplo usa o atributo* `email` *. Você pode usar qualquer identificador exclusivo que seja exposto pelo formato X.509, tenha um tamanho igual ou inferior a 254 caracteres e seja compartilhado pelo serviço de diretório LDAP e pelo Adobe Connect.*

2. Defina a política de logon do Connect

O Adobe Connect precisa usar um endereço de email para o logon do usuário. No Adobe Connect Central, selecione a guia Administração e clique em Usuários e grupos, clique em Editar políticas de logon e senha.

3. Configure o servidor da CA.

O servidor da CA (autoridade de certificação) lida com solicitações de certificados, verifica a identidade do cliente, emite certificados e gerencia uma lista de rejeição de cliente (CRL).

Nesta implementação, a CA aponta para o servidor de diretório LDAP para obter um certificado de cliente. A CA consulta o servidor LDAP em relação às informações do cliente e, caso elas existam e não tenham sido revogadas, o cria na forma de um certificado.

Verifique se o certificado do cliente está instalado e pode ser utilizado, bastando olhar no campo assunto. Ele tem a seguinte aparência:

```
E = adavis@asp.sflab.macromedia.com
CN = Andrew Davis
CN = Users
DC = asp
DC = sflab
DC = macromedia
DC = com
```

4. Configure o Adobe Connect para usar autenticação de cabeçalho HTTP.

No arquivo *[dir_instalação_raiz]*\appserv\web\WEB-INF\web.xml, exclua as barras de comentário do seguinte código:

```
<filter-mapping>
    <filter-name>HeaderAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

Pare o servidor de reunião e o servidor de aplicativos. No arquivo custom.ini do diretório raiz de instalação, adicione a seguinte linha:

```
HTTP_AUTH_HEADER=hah_login
```

Salve o arquivo custom.ini e reinicie o Connect.

5. Configure a lógica do aplicativo F5.

A lógica do aplicativo no F5 analisa o campo de assunto do certificado do cliente para obter o endereço de email. A lógica passa o endereço de email para o Adobe Connect em um cabeçalho HTTP adicional.

O cliente que não possuir um certificado será rejeitado. Se o cliente possuir um certificado, este deverá ser autenticado. Entre os exemplos de mecanismos de autenticação estão o OCSP (Online Certification Status Protocol) e a pesquisa de LDAP.

Assim que o certificado estiver autenticado, analise-o para obter um identificador único conhecido pelo Adobe Connect. Neste exemplo, o certificado válido é analisado para um endereço de email.

A solicitação que inclui a string `session` ou possua o cookie `BREEZESESSION` pode passar sem autenticação, pois já foi autenticada pelo cliente. (O Adobe Connect verifica esses argumentos com uma consulta ao banco de dados.)

Se a solicitação não incluir a string `session` ou o cookie `BREEZESESSION`, o usuário precisará fazer logon no Adobe Connect. Para fazer o logon de um usuário, coloque o identificador exclusivo (neste caso, o endereço de email) no campo `HTTP_AUTH_HEADER` e redirecione a solicitação para a página de logon do Adobe Connect.

O código a seguir é um F5 iRule localizado no perfil HTTPS que lida com as solicitações:

```
set id [SSL::sessionid]
set the_cert [session lookup ssl $id]
set uname [X509::subject $the_cert]
set emailAddr [getfield $uname "emailAddress=" 2]
if { [HTTP::cookie exists BREEZESESSION] } {
    set cookie_payload [HTTP::cookie value BREEZESESSION]
}
elseif { [HTTP::uri] contains "/system/login" }
{
    # Connection has been redirected to the "login page"
    # The email address has been parsed from the certificate
    #
    HTTP::header insert hah_login $emailAddr
}
elseif { [HTTP::uri] contains "session" }
{
    #do nothing, Adobe Connect verifies the token found in session=$token
}
else
{
    # URI encode the current request, and pass it to
    # the Adobe Connect system login page because the client
    # does not have a session yet.
    HTTP::redirect https://[HTTP::host]/system/login/ok?next=[URI::encode
https://[HTTP::host][HTTP::uri]]
}
```

Mais tópicos da Ajuda

"Iniciar e parar o Adobe Connect" na página 81

Proteção da infra-estrutura

Segurança da rede

O Adobe Connect utiliza vários serviços TCP/IP privados para realizar suas comunicações. Esses serviços abrem várias portas e canais que precisam ser protegidos de usuários externos. O Adobe Connect exige que você coloque portas confidenciais atrás de um firewall. O firewall deve suportar a inspeção de pacotes com informações de estado (não apenas a filtragem dos pacotes). Ele deve ter a opção de "recusar todos os serviços por padrão, exceto aqueles explicitamente permitidos". O firewall deve ser no mínimo de base dupla (dual-homed), ou seja, com suporte para duas ou mais interfaces de rede. Essa arquitetura ajuda a impedir que usuários não autorizados violem a segurança do firewall.

A solução mais fácil para proteger o Adobe Connect é bloquear todas as portas no servidor, exceto as portas 80, 1935 e 443. O firewall de um hardware externo fornece uma camada de proteção contra as falhas no sistema operacional. É possível configurar camadas dos firewalls de hardwares para formarem DMZs. Se o servidor for cuidadosamente atualizado pelo departamento de TI com as últimas atualizações de segurança da Microsoft, um software de firewall pode ser configurado para fornecer segurança adicional.

Acesso à intranet

Para que usuários possam acessar o Adobe Connect na intranet, os servidores do Adobe Connect e o banco de dados do Adobe Connect devem estar em uma sub-rede separada, isolada por um firewall. O segmento da rede interna no qual o Adobe Connect está instalado deve usar endereços IP privados (10.0.0.0/8, 172.16.0.0/12 ou 192.168.0.0/16) para tornar difícil aos invasores direcionar o tráfego para um endereço IP público e a partir do IP interno usado como endereço de rede. Para obter mais informações, consulte a RFC 1918. Esta configuração do firewall deve levar em consideração todas as portas do Adobe Connect e se elas estão configuradas para entrada ou saída de tráfego.

Segurança do banco de dados

Independentemente de seu banco de dados estar ou não hospedado no mesmo servidor Adobe Connect, certifique-se de que o banco de dados esteja protegido. Os computadores que hospedam bancos de dados precisam estar em locais fisicamente seguros. Veja abaixo alguns cuidados que devem ser tomados:

- Instale o banco de dados na zona segura da sua intranet.
- Nunca conecte o banco de dados diretamente à Internet.
- Faça backup de todos os dados regularmente e armazene as cópias em um local seguro fora das instalações comerciais.
- Instale as últimas atualizações do servidor do banco de dados.
- Use conexões confiáveis SQL.

Para obter informações sobre como proteger o SQL Server, consulte o site de segurança do Microsoft SQL.

Criar contas de serviços

A criação de uma conta de serviços do Adobe Connect permite que o Adobe Connect seja executado com mais segurança. A Adobe recomenda criar uma conta de serviço e uma conta do serviço SQL Server 2005 Express Edition para o Adobe Connect. Para obter mais informações, consulte os artigos da Microsoft "How to change the SQL Server or SQL Server Agent service account without using SQL Enterprise Manager in SQL Server 2000 or SQL Server Configuration Manager in SQL Server 2005" e "The Services and Service Accounts Security and Planning Guide".

Criar uma conta de serviço

1 Crie uma conta local, com o nome de ConnectService, que não contenha nenhum grupo padrão.

2 Ative os serviços Adobe Connect Service, o Flash Media Administration Server e o Flash Media Server (FMS) para essa nova conta.

3 Atribua "Controle total" para esta chave de registro:

```
HKLM\SYSTEM\ControlSet001\Control\MediaProperties\PrivateProperties\Joystick\Winmm
```

4 Atribua "Controle total" para as pastas NTFS no caminho da raiz do Adobe Connect (c:\breeze, por padrão).

As subpastas e arquivos devem receber as mesmas permissões. Os caminhos dos clusters devem ser modificados em cada nó do computador.

5 Atribua os seguintes direitos de logon para a conta ConnectService:

Fazer logon como um serviço — SeServiceLogonRight

Criar uma conta do serviço SQL Server 2005 Express Edition

1 Crie uma conta local, com o nome de ConnectSqlService, que não contenha nenhum grupo padrão.

2 Altere a conta do SQL Server 2005 Express Edition Service de LocalSystem para ConnectSqlService.

3 Atribua "Controle total" para as seguintes chaves de registro na conta ConnectSqlService:

```
HKEY_LOCAL_MACHINE\Software\Clients\Mail
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\80
HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft SQL Server\[databaseInstanceName]
```

Execute a etapa a seguir em todos os nós do cluster. A permissão de controle total se aplica a todas as chaves secundárias de uma instância com nome definido do banco de dados.

4 Atribua "Controle total" para pastas do banco de dados na conta ConnectSqlService. As subpastas e arquivos também devem receber as mesmas permissões. Os caminhos dos clusters devem ser modificados em cada nó do computador.

5 Atribua os seguintes direitos de usuário para a conta de serviços ConnectSqlService:

Atuar como parte do sistema operacional — SeTcbPrivilege; Ignorar a verificação completa — SeChangeNotify; Bloquear páginas na memória — SeLockMemory; Fazer logon como um trabalho em lotes — SeBatchLogonRight; Fazer logon como um serviço — SeServiceLogonRight; Substituir um token no nível de processo — SeAssignPrimaryTokenPrivilege

Proteção das instalações com apenas um servidor

O fluxo de trabalho a seguir resume o processo de configuração e a proteção do Adobe Connect em um único computador. Ele parte do princípio de que o banco de dados será instalado no mesmo computador e que os usuários acessarão o Adobe Connect pela Internet.

1. Instale um firewall.

Como você está permitindo o acesso de usuários ao Adobe Connect pela Internet, o servidor fica vulnerável a ataques de invasores. O firewall permite bloquear o acesso ao servidor e controlar as comunicações que ocorrem entre a Internet e o servidor.

2. Configure o firewall.

Após instalar o firewall, configure-o conforme descrito a seguir:

- Portas de entrada (dados recebidos da Internet): 80, 443 e 1935.
- Porta de saída (dados enviados para o servidor de mensagens): 25.
- Use apenas o protocolo TCP/IP.

  Como o banco de dados está localizado no mesmo servidor Adobe Connect, não é preciso abrir a porta 1434 no firewall.

3. Instale o Adobe Connect.

4. Verifique se os aplicativos do Adobe Connect estão funcionando.

Após instalar o Adobe Connect, verifique se ele está funcionando corretamente da Internet e da rede local.

5. Teste o firewall.

Após instalar e configurar o firewall, verifique se ele está funcionando corretamente. Para testar o firewall, tente usar as portas bloqueadas.

Proteção dos clusters

Os próprios sistemas de clusters (com vários servidores) são mais complexos que as configurações com apenas um servidor. Um cluster do Adobe Connect pode estar localizado em um centro de dados ou distribuído geograficamente entre os vários centros de operações da rede. É possível instalar e configurar servidores que hospedam o Adobe Connect em diferentes locais e sincronizá-los por meio da replicação do banco de dados.

Nota: *Os clusters devem usar o Microsoft SQL Server 2005 Standard Edition, e não o mecanismo de banco de dados incorporado.*

Veja a seguir algumas dicas importantes para a segurança dos clusters:

Redes privadas A solução mais simples para clusters em um único local é criar uma sub-rede extra para o sistema Adobe Connect. Essa estratégia oferece um alto nível de segurança.

Softwares de firewalls locais Para os servidores Adobe Connect que estão localizados em um cluster, mas compartilham uma rede pública com outros servidores, pode ser apropriado usar um firewall de software em cada servidor.

Sistemas de VPN (rede privada virtual) Em instalações com vários servidores, que hospedam o Adobe Connect em diferentes locais físicos, pode ser vantajoso usar um canal criptografado para se comunicar com os servidores remotos. Muitas revendedoras de softwares e hardwares oferecem a tecnologia VPN para proteger comunicações com servidores remotos. O Adobe Connect se vale dessa segurança externa quando o tráfego de dados precisa ser criptografado.

Dicas e recursos de segurança

Práticas recomendadas de segurança

A lista de verificação a seguir descreve as práticas recomendadas à proteção do sistema Adobe Connect:

Use o padrão SSL para proteger o tráfego na rede. Você pode proteger a conexão com o servidor de reunião, com o servidor de aplicativos ou com ambos.

Execute apenas os serviços necessários. Não execute aplicativos como controladores de domínios, servidores Web ou servidores FTP no mesmo computador do Adobe Connect. Para minimizar a chance de que outro aplicativo possa ser usado para comprometer o servidor, reduza o número de aplicativos e serviços executados no computador que hospeda o Adobe Connect.

Atualize a segurança do sistema operacional. Consulte regularmente as atualizações de alta prioridade, para corrigir falhas na segurança e instalar os patches necessários. Um firewall elimina alguns desses problemas de segurança. Em geral, mantenha os servidores sempre atualizados com todos os patches de segurança aprovados pela Microsoft e pelos fornecedores de outras plataformas relevantes.

Proteja os sistemas de host. Antes de armazenar informações importantes nos servidores, informe-se sobre a segurança física dos seus sistemas. O Adobe Connect se vale da segurança do sistema de host para se proteger contra invasores. Portanto, os servidores precisam estar protegidos quando informações privadas e confidenciais estiverem expostas a riscos. O Adobe Connect foi desenvolvido para usufruir dos recursos nativos do ambiente em que se encontra, como a criptografia do sistema de arquivos.

Use senhas seguras. Senhas seguras protegem os dados. Os administradores do Adobe Connect podem configurar as políticas de logon e de senha no Connect Central. Geralmente, as instalações do Adobe Connect usam o Microsoft SQL Server 2005 Standard Edition, que também exige a proteção de senhas seguras.

Usar LDAP para autenticação É a melhor prática usar o LDAP para autenticação do Connect.

Realize auditorias de segurança regularmente. Faça auditorias no seu sistema periodicamente, para verificar se todos os recursos de segurança continuam operando corretamente. Por exemplo, você pode fazer varreduras das portas para testar o firewall.

Recursos e referências de segurança

Os recursos a seguir ajudam a proteger seus servidores:

Segurança da rede O SANS Institute (Instituto de administração de sistemas, gerenciamento de redes e segurança) é uma organização para a cooperação em pesquisa e educação que inclui administradores de sistema, profissionais de segurança e administradores de rede. Ele oferece cursos sobre segurança e também certificados em segurança de rede.

Segurança do SQL Server A página de recursos de segurança do SQL Server, no site da Microsoft, contém informações sobre a segurança do SQL Server.

Ferramentas O Nmap é um ótimo programa de varredura de portas que informa quais portas estão sendo usadas pelo sistema. Ele é distribuído gratuitamente com base na GNU Public License (GPL).

Nota: *A eficácia das medidas de segurança é determinada por vários fatores, como as medidas de segurança fornecidas pelo servidor e pelo software de segurança instalado. O software Adobe Connect não foi desenvolvido para proteger o seu servidor ou as informações nele armazenadas. Para obter mais informações, consulte os termos de Isenção de Responsabilidade, no Contrato de Licença aplicável fornecido com o Adobe Connect.*

Capítulo 5: Administração do Adobe Connect

A administração do Adobe Connect envolve os seguintes procedimentos:

- Gerenciamento e monitoramento de arquivos de registro para manter o sistema atualizado
- Manutenção do espaço em disco
- Backup de dados
- Criação e geração de relatórios de uso

Iniciar e parar os servidores

Iniciar e parar o Adobe Connect

O Connect pode ser iniciado ou parado no menu Iniciar, na janela Serviços ou na linha de comando. Verifique se o banco de dados está em execução antes de iniciar o Connect.

Parar o Connect no menu Iniciar

1 Clique em Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Application Server.

2 Clique em Iniciar > Programas > Adobe Connect Server > Parar o Connect Meeting Server.

Iniciar o Adobe Connect no menu Iniciar

1 Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Meeting Server.

2 Clique em Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Application Server.

Parar o Adobe Connect na janela Serviços

1 Para abrir a janela Serviços, clique em Iniciar > Painel de controle > Ferramentas administrativas > Serviços.

2 Pare o serviço Adobe Connect Enterprise Service.

3 Pare o serviço Flash Media Server (FMS).

4 Pare o serviço Flash Media Server Administration Server.

Iniciar o Adobe Connect na janela Serviços

1 Para abrir a janela Serviços, clique em Iniciar > Painel de controle > Ferramentas administrativas > Serviços.

2 Inicie o serviço Flash Media Server (FMS).

3 Inicie o serviço Flash Media Server Administration Server.

4 Inicie o serviço Adobe Connect Service.

Parar o Adobe Connect na linha de comando

1 Para abrir a janela Executar, clique em Iniciar > Executar. Digite **cmd** para abrir um prompt de comando.

2 Vá para o diretório *[Diretório_deInstalação_Raiz]*\appserv\win32.

3 Digite o seguinte comando para parar o Adobe Connect:

```
net stop ConnectPro
```

4 Digite o seguinte comando para parar o Flash Media Server:

```
net stop FMS
```

5 Digite o seguinte comando para parar o Flash Media Server Administration Server:

```
net stop FMSAdmin
```

Iniciar o Adobe Connect na linha de comando

1 Para abrir a janela Executar, clique em Iniciar > Executar. Digite **cmd** para abrir um prompt de comando.

2 Vá para o diretório *[DiretóriodeInstalaçãoRaiz]*\appserv\win32.

3 Digite o seguinte comando para iniciar o Flash Media Server:

```
net start FMS
```

4 Digite o seguinte comando para iniciar o Flash Media Server Administration Server:

```
net start FMSAdmin
```

5 Digite o seguinte para iniciar o Adobe Connect:

```
net start ConnectPro
```

Iniciar e parar o Adobe Connect Presence Service

É possível iniciar e parar o Adobe Connect Presence Service no menu Iniciar ou na janela Serviços. Inicie o Adobe Connect Presence Service somente se seu sistema Adobe Connect estiver integrado ao Microsoft Live Communications Server ou ao Office Communications Server.

Mais tópicos da Ajuda

"Integração com o Microsoft Live Communications Server 2005 e Microsoft Office Communications Server 2007" na página 59

Parar o serviço de presença no menu Iniciar

❖ Escolha Iniciar > Programas > Adobe Connect Server > Parar o Connect Presence Service.

Iniciar o serviço de presença no menu Iniciar

❖ Escolha Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Presence Service.

Parar, iniciar ou reiniciar o serviço de presença na janela Serviços

1 Para abrir a janela Serviços, clique em Iniciar > Painel de controle > Ferramentas administrativas > Serviços.

2 Selecione o Adobe Connect Presence Service.

3 Escolha Iniciar, Parar ou Reiniciar o serviço.

Iniciar e parar o Adobe Connect Telephony Service

Você pode iniciar e parar o Adobe Connect Telephony Service da janela Serviços.

1 Para abrir a janela Serviços, clique em Iniciar > Painel de controle > Ferramentas administrativas > Serviços.

2 Selecione o Adobe Connect Telephony Service.

3 Escolha Iniciar, Parar ou Reiniciar o serviço.

Iniciar e parar o Flash Media Gateway

Você pode iniciar e parar o Flash Media Gateway pela janela Serviços ou pela linha de comando. Verifique se o Adobe Connect Server está sendo executado antes de iniciar o Flash Media Gateway.

Iniciar e parar o Flash Media Gateway pela janela Serviços

1 Para abrir a janela Serviços, clique em Iniciar > Painel de controle > Ferramentas administrativas > Serviços.

2 Selecione o serviço Flash Media Gateway.

3 Escolha Iniciar, Parar ou Reiniciar o serviço

Iniciar e parar o Flash Media Gateway pela linha de comando

1 Para abrir a janela Executar, clique em Iniciar > Executar. Digite **cmd** para abrir um prompt de comando.

2 Digite o seguinte comando para iniciar o Flash Media:

```
net start fmg
```

3 Digite o seguinte comando para parar o Flash Media:

```
net stop fmg
```

Iniciar e parar o Adobe Connect Edge Server

O Adobe Connect pode ser iniciado ou o Adobe Connect Edge Server pode ser parado no menu Iniciar, na janela Serviços ou na linha de comando.

Parar o Adobe Connect Edge Server no menu Iniciar

❖ Escolha Iniciar > Programas > Adobe Connect Edge Server > Interromper o Connect Edge Server.

Iniciar o Adobe Connect Edge Server no menu Iniciar

❖ Escolha Iniciar > Programas > Adobe Connect Edge Server > Iniciar o Connect Edge Server.

Parar o Adobe Connect Edge Server na janela Serviços

1 Para abrir a janela Serviços, clique em Iniciar > Configurações > Painel de controle > Ferramentas administrativas > Serviços.

2 Pare o serviço Flash Media Server (FMS).

3 Pare o serviço Flash Media Server Administration Server.

Iniciar o Adobe Connect Edge Server 7 na janela Serviços

1 Para abrir a janela Serviços, clique em Iniciar > Configurações > Painel de controle > Ferramentas administrativas > Serviços.

2 Inicie o serviço Flash Media Server Administration Server.

3 Inicie o serviço Flash Media Server (FMS).

Parar o Adobe Connect Edge Server na linha de comando

1 Para abrir a janela Executar, clique em Iniciar > Executar. Digite **cmd** para abrir um prompt de comando.

2 Digite o seguinte comando para parar o Flash Media Server:

```
net stop FMS
```

3 Digite o seguinte comando para parar o Flash Media Server Administration Server:

```
net stop FMSAdmin
```

Iniciar o Adobe Connect Edge Server na linha de comando

1 Para abrir a janela Executar, clique em Iniciar > Executar. Digite **cmd** para abrir um prompt de comando.

2 Digite o seguinte comando para iniciar o Flash Media Server Administration Server:

```
net start FMSAdmin
```

3 Digite o seguinte comando para iniciar o Flash Media Server:

```
net start FMS
```

Gerenciamento e monitoramento de arquivos de registro

Sobre os arquivos de registro

Use os arquivos de registro do Adobe Connect para visualizar informações sobre os eventos que ocorrem durante a operação. Você pode usar as informações nos arquivos de registro para criar mecanismos de monitoramento e relatórios e para solucionar problemas. Os arquivos de registro fornecem informações sobre as atividades dos usuários e o desempenho do servidor. Por exemplo, os arquivos de registro podem indicar o motivo por que o acesso foi negado a um usuário durante o logon ou o motivo por que houve falha de uma conexão telefônica.

Os arquivos de registro do Adobe Connect estão na pasta *PastadaInstalaçãoRaiz*\logs.

Os arquivos de registro do Apache Tomcat estão na pasta *PastadaInstalaçãoRaiz*\logs\tomcat.

Configuração de arquivos de registro

O Adobe Connect usa a ferramenta Apache log4j. Use o arquivo *PastadaInstalaçãoRaiz*\appserv\conf\log4j.xml para configurar o registro em log. Para obter mais informações, consulte Primer de configuração XML Log4j.

Exemplo de entrada no arquivo de registro

O exemplo de entrada a seguir, do arquivo access.log, inclui um cabeçalho, uma lista dos campos usados na entrada do registro e os dados específicos desta entrada de registro:

```
#Version: 1.0
#Start-Date: 2010-10-30 17:09:24 PDT
#Software: Adobe Connect Server
#Date: 2010-04-30
#Fields: date time x-comment x-module x-status x-severity x-category x-user x-access-request
time-taken db-logical-io db-transaction-update-count
2006-10-30 18:12:50 Not logged in. PRINCIPAL NO_ACCESS_NO_LOGIN W A PUBLIC
{cookie=breezxnb5pqusyshfgttt, ip=138.1.21.100} GET http://joeuser.adobe.com&mode=xml 0 20/5 0
```

A tabela a seguir explica a mesma entrada:

Campo	Dados	Descrição
date	30-10-2010	A data em que o evento registrado ocorreu.
time	18:12:50	A hora em que o evento registrado ocorreu.
x-comment	Não conectado.	Indica que um usuário não conseguiu fazer logon no servidor de aplicativos.
x-module	PRINCIPAL	O evento ocorreu no módulo Principal, no servidor de aplicativos.
x-status	NO_ACCESS_NO_LOGIN	Indica que o usuário não conseguiu fazer logon.
x-severity	W	Identifica a gravidade do evento como um aviso (W - warning).
x-category	A	Indica que o evento é um problema de acesso (A) (registrado no arquivo access.log).
x-user	PUBLIC	O usuário atual, neste caso, um convidado não identificado ou usuário público.
x-access-request	http://joeuser.adobe.com&mode=xml	Fonte da solicitação.
time-taken	0	Nenhum tempo foi necessário ao processamento desta solicitação.
db-logical-io	20/5	Foram necessárias 20 leituras do banco de dados e cinco linhas de dados foram retornadas.
db-transaction-update-count	0	Nenhuma linha foi adicionada ao banco de dados no processamento desta solicitação.

Formato de arquivos de registro

Os arquivos de registro usam o formato de arquivo de registro estendido W3C, sendo possível utilizar qualquer editor de texto para lê-los.

Campos de registro nos arquivos access.log e error.log

Cada entrada do registro contém 11 campos de registro, que fornecem informações sobre o tipo de evento ocorrido, onde ocorreu, sua gravidade, entre outros dados relevantes:

Campo	Formato	Descrição
date	AAAA/MM/DD	Data em que a transação foi concluída.
time	HH:MM:SS	Hora local do computador em que a transação foi concluída.
x-comment	String	Contém informações legíveis por humanos sobre a entrada no registro. Este campo é sempre apresentado como o campo mais à esquerda.
x-module	String	Indica onde o erro ocorreu.
x-status	String	Indica o evento ocorrido.
x-severity	Texto (um caractere)	Indica se o evento registrado é crítico (C), erro (E), aviso (W) ou informação (I).
x-category	Texto (um caractere)	Indica se a entrada do registro representa um evento de acesso (A) ou do sistema (S).
x-user	String	Texto que representa o usuário atual. Aplica-se somente se x-category for acesso (A). Caso contrário, o campo é definido como um único hífen (-), que denota um campo não usado.

Campo	**Formato**	**Descrição**
x-access-request	String	Texto que representa a solicitação de acesso. Esse texto pode ser um URL ou um nome da API com parâmetros. Aplicável somente se x-category for um acesso (A). Caso contrário, este campo é definido com um hífen, que denota um campo não utilizado.
time-taken	Número	Tempo necessário para processar a solicitação (em segundos). Aplicável somente se x-category for um acesso (A). Caso contrário, este campo é definido com um hífen, que denota um campo não utilizado.
db-logical-io	String	Número de leituras no banco de dados necessárias para processar a solicitação e número de linhas retornadas no formato <reads>/<rows>.
db-transaction-update-count	String	Número de linhas atualizadas nas transações durante o processamento das solicitações. Se a solicitação usar mais de uma transação, esse valor será a soma de todas as atualizações.

Entradas de campos de módulos

Um módulo é um componente do servidor que gerencia algum conjunto de operações relacionadas. Cada módulo pertence ao servidor de aplicativos ou ao servidor de reunião. O campo x-module indica onde o evento registrado ocorreu:

Entrada no registro para o campo x-module	**Descrição**	**Servidor**
ACCESS_KEY	Gerencia as chaves de acesso.	Servidor de aplicativos
ACCOUNT	Gerencia operações de conta.	Servidor de aplicativos
ACL	Gerencia operações relacionadas à ACL.	Servidor de aplicativos
AICC	Gerencia todas as comunicações AICC entre o servidor e o conteúdo.	Servidor de aplicativos
BUILDER	Executa compilações de SCO.	Servidor de aplicativos
Client	Métodos de cliente.	Servidor de reunião
CLUSTER	Gerencia todas as operações relacionadas a clusters.	Servidor de aplicativos
CONSOLE	Gerencia todas as operações relacionadas ao console.	Servidor de aplicativos
Content	Compartilhado, pod.	Servidor de reunião
DB	Representa o banco de dados.	Servidor de aplicativos
EVENT	Gerencia todas as operações relacionadas a eventos.	Servidor de aplicativos
HOSTED_MANAGER	Gerencia contas do sistema (criar, atualizar, excluir, configurações etc.).	Servidor de aplicativos
MEETING	Gerencia todas as operações relacionadas a reuniões.	Servidor de aplicativos
Misc	Módulo Diversos.	Servidor de reunião
NOTIFICATION	Gerencia todas as operações de email.	Servidor de aplicativos
PERMISSION	Gerencia todas as operações relacionadas a permissões.	Servidor de aplicativos
Poll	Pesquisa, pod.	Servidor de reunião
PLATFORM_FRAMEWORK	Representa a estrutura da plataforma.	Servidor de aplicativos
PRINCIPAL	Gerencia todas as operações relacionadas ao principal.	Servidor de aplicativos

Entrada no registro para o campo x-module	Descrição	Servidor
REPORT	Representa relatórios.	Servidor de aplicativos
Room	Gerencia a inicialização e o encerramento das salas de reuniões.	Servidor de reunião
RTMP	Representa RTMPHandler.	Servidor de aplicativos
SCO	Gerencia todas as operações relacionadas a SCO.	Servidor de aplicativos
SEARCH	Gerencia todas as operações relacionadas a pesquisa.	Servidor de aplicativos
START_UP	Representa o componente de inicialização.	Servidor de aplicativos
TELEPHONY	Gerencia todas as operações relacionadas a telefonia.	Servidor de aplicativos
TRACKING	Gerencia todas as operações relacionadas a transcrições.	Servidor de aplicativos
TRAINING	Gerencia todas as operações relacionadas a treinamento.	Servidor de aplicativos

Entradas de campos de comentário e status

Os campos x-comment e x-status indicam o tipo de evento ocorrido. O campo x-status fornece um código para cada evento registrado. O campo x-comment fornece uma descrição legível por humanos de cada evento registrado.

A tabela a seguir lista os códigos de status, o comentário associado a cada um deles e uma explicação de cada evento registrado:

Entrada do registro para o campo x-status	Entrada do registro para o campo x-comment	Descrição
ACCESS_DENIED	Client trying to access protected method. Access is denied. {1}	Registrado quando o cliente tenta acessar um método protegido.
BECAME_MASTER	Server {1} has been designated the master.	Registrado quando o agendador é encerrado e este servidor se torna o agendador.
CLUSTER_CON_BROKEN	Server {1} unable to reach {2} on port {3} to perform cluster operations.	Registrado quando o Adobe Connect não tem acesso a outro servidor no cluster.
CLUSTER_FILE_TRANSFER_ERROR	Unable to transfer {1} from server {2}.	Registrado quando um erro é emitido durante a transferência de um arquivo.
CONNECT	New client connecting: {1}	Registrado quando um novo cliente se conecta.
CONNECT_WHILE_GC	Connecting while the application is shutting down - forcing shutdown.	Registrado quando o cliente tenta se conectar enquanto o aplicativo está sendo encerrado.
DB_CONNECTION_ERROR	Unable to connect to database {1}.	Registrado quando o Adobe Connect não tem acesso ao banco de dados.
DB_CONNECTION_TIME_OUT	Timed out waiting for database connection.	Registrado quando a conexão com o banco de dados é muito demorada.
DB_VERSION_ERROR	Database {1} is incompatible with the current version of Adobe Connect.	Registrado quando o banco de dados está desatualizado.
DISCONNECT	A client is leaving. Details: {1}	Registrado quando o cliente se desconecta.

Entrada do registro para o campo x-status	**Entrada do registro para o campo x-comment**	**Descrição**
EXT_ERROR	External error thrown by a third party.	Registrado quando o código externo emite um erro.
FMS_CON_BROKEN	Health check failed due to broken FMS service connection.	Registrado quando a conexão de serviço é perdida.
FMS_NOT_FOUND	Unable to connect to FMS at startup.	Registrado quando o Adobe Connect não consegue estabelecer a conexão de serviço na inicialização.
INTERNAL_ERROR	Internal error occurred.	Registrado quando um erro interno é emitido.
INVALID	-	Registrado quando uma operação inválida é tentada.
INVALID_DUPLICATE	Value {1} is a duplicate in the system.	Registrado quando o valor inserido duplica um valor no sistema.
INVALID_FORMAT	Field {1} of type {2} is invalid.	Valor especificado é inválido para este campo.
INVALID_ILLEGAL_OPERATION	Illegal operation performed.	A operação solicitada é ilegal.
INVALID_ILLEGAL_PARENT	-	Registrado quando a ACL tem um pai inválido. Por exemplo, se a pasta A está dentro da pasta B, a pasta B não pode estar na pasta A.
INVALID_MISSING	Field {1} of type {2} is missing.	Valor obrigatório ausente neste campo.
INVALID_NO_SUCH_ITEM	Value {1} is an unknown in the system.	O item solicitado não existe.
INVALID_RANGE	The specified value must be between {1} and {2}.	Registrado quando o valor inserido está fora do intervalo.
INVALID_TELEPHONY_FIELD	Telephony authentication values were not validated by the service provider.	O provedor de serviços não pôde validar a conta de telefonia.
INVALID_VALUE_GTE	The specified value must be greater than or equal to {1}.	Registrado quando o valor inserido está fora do intervalo.
INVALID_VALUE_LTE	The specified value must be less than or equal to {1}.	Registrado quando o valor inserido está fora do intervalo.
KILLING_LONG_CONNECTION	Client has been in the room for 12 hours, disconnecting.	Registrado quando a conexão do cliente é terminada após o esgotamento do tempo limite.
LICENSE_EXPIRED	Your license has expired and your account will be disabled on {1}. Please upload a new license file through the console manager to continue using Adobe Connect.	Registrado quando o cliente está usando o Adobe Connect durante o período de cortesia e o acesso está prestes a ser parado.
LICENSE_EXPIRY_WARNING	Your license will expire on {1}. Please upload a new license file through the console manager to continue using Adobe Connect.	Registrado quando a licença está a 15 dias ou menos da data de expiração.
MASTER_THREAD_TIMED_OUT	Master thread has not reported progress in {1} milliseconds.	A linha do agendador não está em execução.
MEETING_BACKUP_END	Server {1} is no longer the backup for room {2}.	O backup da reunião terminou.
MEETING_BACKUP_START	Server {1} is now the backup for room {2}.	O backup da reunião foi iniciado.

Entrada do registro para o campo x-status	**Entrada do registro para o campo x-comment**	**Descrição**
MEETING_FAILOVER	Meeting {1} failed over to {2}.	Registrado quando uma reunião é redirecionada para este servidor.
MEETING_TMP_READ	Meeting template {1} read for room {2}.	Modelo lido a partir da reunião.
MEETING_TMP_WRITTEN	Meeting template {1} written to room {2}.	Modelo gravado na reunião.
NO_ACCESS_ACCOUNT_EXPIRED	Your account has expired.	A conta acessada expirou.
NO_ACCESS_DENIED	Permission check failed.	Erro de verificação de permissão.
NO_ACCESS_LEARNER	No permission to take courses.	É preciso ser um membro do grupo de alunos para fazer um curso.
NO_ACCESS_LEARNING_PATH_BLOCKED	You have not fulfilled a prerequisite or preassessment.	Erro de pré-requisito ou pré-avaliação.
NO_ACCESS_NO_EXTERNAL_USER_MODIFICATION	External users cannot be modified.	O usuário não está autorizado a modificar os usuários do LDAP.
NO_ACCESS_NO_LICENSE_FILE	Your license file has not been uploaded.	Arquivo de licença não encontrado.
NO_ACCESS_NO_LOGIN	Not logged in.	Erro emitido quando o usuário não estava conectado.
NO_ACCESS_NO_QUOTA	A {1} quota error occurred for account {2} with limit {3}.	Cota preenchida.
NO_ACCESS_NO_RETRY	You have reached the max limit and can not take the course again.	O usuário ultrapassou o limite de novas entradas no curso.
NO_ACCESS_NO_SERVER	Server not available	O servidor solicitado não está disponível.
NO_ACCESS_NOT_AVAILABLE	The requested resource is unavailable.	Registrado quando o recurso solicitado não está disponível.
NO_ACCESS_NOT_SECURE	SSL request made on a non-SSL server.	Solicitação segura feita em um servidor não seguro.
NO_ACCESS_PASSWORD_EXPIRED	Your password has expired.	Registrado quando uma senha de usuário expirou.
NO_ACCESS_PENDING_ACTIVATION	Your account has not been activated yet.	A conta ainda não foi ativada.
NO_ACCESS_PENDING_LICENSE	Your account activation is pending a license agreement.	A conta não pode ser usada até que o contrato de licença seja lido.
NO_ACCESS_SCO_EXPIRED	The course you tried to access is no longer available.	A data de fim do curso já passou.
NO_ACCESS_SCO_NOT_STARTED	Course is not open yet.	Data de início do curso não atingido.
NO_ACCESS_WRONG_ZONE	Content accessed from wrong zone.	Emitido quando o conteúdo ou o usuário acessam um servidor na zona incorreta.
NO_DATA	Permission check failed.	A consulta não retornou nenhum dado.
NO_DISKSPACE	Health check failed due to lack of disk space.	Registrado quando a conta está sem espaço em disco.
NOT_AVAILABLE	Requested resource is not available.	Erro emitido quando o recurso não está disponível.
OK	-	Solicitação processada com êxito.

Entrada do registro para o campo x-status	Entrada do registro para o campo x-comment	Descrição
OPERATION_SIZE_ERROR	Operation too large to complete.	Registrado quando a operação não pode ser concluída devido ao tamanho.
REQUEST_RETRY	Unable to process request. Please try again.	Falha da solicitação.
RESPONSE_ABORTED	Client that made request is not available to receive response.	Registrado quando o usuário fecha o navegador antes de o servidor enviar a resposta de volta.
RTMP_SVC_BLOCKED	Adobe Connect service request blocked from {1} because the server has not fully started up yet.	O SCO solicitou a conexão de serviço, mas o servidor ainda está sendo inicializado.
RTMP_SVC_CLOSED	Adobe Connect service connection closed for {1}.	Conexão de serviço do SCO fechada.
RTMP_SVC_REQUEST	Adobe Connect service request received from {1}.	O SCO solicitou conexão de serviço.
RTMP_SVC_START	Adobe Connect service connection established with {1}.	Conexão de serviço estabelecida com o SCO.
SCRIPT_ERROR	Run-Time Script Error. Details: {1}	Registrado quando um erro de script é detectado.
SERVER_EXPIRED	Health check failed due to server expiry (expiry date={1}, current time={2}).	Registrado quando o servidor não é aprovado na verificação de integridade antes do tempo limite.
SOME_ERRORS_TERMINATED	Some actions terminated with an error.	Registrado quando um erro causa o término de algumas ações.
START_UP_ERROR	Start up error: {1}.	Registrado quando uma exceção é emitida durante a inicialização.
START_UP_ERROR_UNKNOWN	Unable to start up server. Adobe Connect might already be running.	Registrado quando um erro desconhecido é emitido durante a inicialização. JRUN imprime o erro.
TEL_CONNECTION_BROKEN	Telephony connection {1} was unexpectedly broken.	Registrado quando a conexão de telefonia é perdida.
TEL_CONNECTION_RECOVERY	Telephony connection {1} was reattached to conference {2}.	Registrado quando o Adobe Connect recupera a conexão com a conferência.
TEL_DOWNLOAD_FAILED	Unable to download {1} for archive {2}.	Registrado quando o tempo limite se esgota durante o download dos arquivos de áudio de telefonia.
TOO_MUCH_DATA	Multiple rows unexpectedly returned.	Registrado quando uma operação retorna mais dados que o esperado.
UNKNOWN_TYPE	{1}	Registrado quando o tipo de variável é desconhecido.

Nota: *Na tabela acima, {1} e {2} são variáveis que são substituídas pelo valor na entrada do registro.*

Entradas de campos de gravidade

O campo x-severity indica a gravidade de uma condição, o que ajuda a determinar o nível de resposta apropriado.

Entrada no registro para x-severity	Significado	Ação sugerida	Exemplo
C	Critical (Crítica)	Configurar ferramentas de monitoração de terceiros para alertar por pager quando uma entrada de registro com este nível de gravidade ocorrer.	Banco de dados inacessível. Não é possível iniciar ou finalizar um processo. Uma falha está afetando o sistema.
E	Erro	Configure ferramentas de monitoração de terceiros para enviar um email quando uma entrada de registro com este nível de gravidade ocorrer.	Adobe® Premiere® não acessível. Falha de conversão. Uma falha está afetando um usuário ou conta, mas não todo o sistema.
W	Aviso	Gerar e revisar relatórios periódicos para identificar possíveis aprimoramentos operacionais ou do produto.	O uso do disco ou da memória excedeu o limite especificado.
I	Informações	Revisar as entradas do registro para fins de auditoria ou RCA.	Servidor iniciado, parado ou reiniciado.

Entradas de campos de categoria

O campo x-category indica se o evento se relaciona a problemas de acesso (A) ou a problemas do sistema em geral (S). Todas as entradas da categoria A aparecem no arquivo access.log, e todas as entradas da categoria S aparecem no arquivo error.log.

Entrada do registro para o campo x-category	Significado	Descrição
A	acesso	O código de status está relacionado a problemas de acesso. Registrado no arquivo access.log.
S	sistema	O código de status está relacionado a problemas do sistema em geral. Registrado no arquivo error.log.

Manutenção do espaço em disco

Sobre a manutenção do espaço em disco

O sistema do Adobe Connect deve ter no mínimo 1 GB de espaço livre. O Adobe Connect não tem nenhuma ferramenta incorporada para monitorar o espaço em disco. O administrador precisa monitorar o espaço em disco com utilitários do sistema operacional ou ferramentas de terceiros.

O conteúdo pode ser armazenado no servidor que hospeda o Adobe Connect, em volumes externos de armazenamento compartilhado ou em ambos.

Mais tópicos da Ajuda

“Configuração do armazenamento compartilhado” na página 52

Manter espaço em disco nos servidores Adobe Connect

❖ Execute um dos procedimentos a seguir:

- Use o Adobe Connect Central para excluir conteúdo não utilizado. Consulte Excluir um arquivo ou pasta.
- Substituir o disco do servidor por um maior.

Nota: *Se o espaço livre em disco no servidor cair para menos de 1 GB, o servidor pára.*

Manter espaço em disco em dispositivos de armazenamento compartilhados

❖ Monitore o dispositivo principal de armazenamento compartilhado quanto ao espaço livre e aos nós do sistema de arquivos disponíveis. Se qualquer deles cair para menos de 10%, adicione mais armazenamento ao dispositivo ou adicione outro dispositivo de armazenamento compartilhado.

Nota: *10% é o valor recomendado. Além disso, se estiver usando armazenamento compartilhado, defina o valor máximo do tamanho do cache no Console de gerenciamento de aplicativos para evitar que o cache preencha o disco.*

Limpar o cache do Edge Server

A Adobe recomenda criar uma tarefa programada semanalmente para limpar o cache do servidor de borda. É uma boa idéia executar a tarefa durante os horários de pouco movimento, como as manhãs de domingo.

1 Crie um arquivo cache.bat para excluir o diretório do cache. A entrada nesse arquivo precisa usar a seguinte sintaxe:

```
del /Q /S [cache directory]\*.*
```

O diretório de cache padrão é C:\breeze\edgeserver\win32\cache\http. Para excluir o cache, use o seguinte comando:

```
del /Q /S c:\breeze\edgeserver\win32\cache\http\*.*
```

2 Selecione Iniciar > Programas > Adobe Connect Edge Server > Parar o Adobe Connect Edge Server.

3 Execute o arquivo cache.bat e verifique se ele exclui arquivos no diretório de cache.

Nota: *A estrutura de diretório permanece e quaisquer arquivos bloqueados pelo servidor de borda não são excluídos.*

4 Selecione Iniciar > Programas > Adobe Connect Edge Server > Iniciar o Adobe Connect Edge Server.

5 Selecione Iniciar > Painel de controle > Tarefas agendadas > Adicionar tarefa agendada.

6 Selecione cache.bat como o novo arquivo para execução.

7 Repita esse procedimento para cada servidor de borda.

Backup de dados

Sobre o backup de dados

Há três tipos de dados cujo backup precisa ser feito a intervalos regulares: conteúdo (todos os arquivos armazenados nas bibliotecas), configurações e dados do banco de dados.

Se você não estiver usando dispositivos de armazenamento compartilhado, todo o conteúdo nas bibliotecas será armazenado na pasta *[DiretóriodeInstalaçãoRaiz]*\content (C:\breeze\content, por padrão). As configurações são armazenadas no arquivo custom.ini na pasta da instalação raiz (C:\breeze, por padrão).

O backup de um banco de dados cria uma duplicata dos dados no banco de dados. Backups de bancos de dados programados a intervalos regulares podem permitir a recuperação de muitas falhas, inclusive falhas de mídia, erros de usuário e perda permanente de um servidor. Faça o backup do banco de dados diariamente.

Também é possível usar backups para copiar um banco de dados de um servidor para outro. É possível recriar todo o banco de dados a partir de um backup em uma etapa, restaurando o banco de dados. O processo de restauração substitui o banco de dados existente ou cria o banco de dados caso ele não exista. O banco de dados restaurado corresponde ao estado do banco de dados no momento em que o backup foi feito, com exceção das transações não confirmadas.

Os backups são criados em dispositivos de backup, como em disco ou fita. É possível usar um utilitário do SQL Server para configurar backups. Por exemplo, você pode substituir backups desatualizados ou incluir novos backups na mídia de backup.

Siga as práticas recomendadas ao fazer o backup do banco de dados:

- Programe um backup noturno.
- Mantenha os backups em um local seguro, de preferência em uma localidade diferente daquela em que os dados residem.
- Guarde os backups mais antigos por um período designado, para o caso de o backup mais recente sofrer danos, ser destruído ou perdido.
- Estabeleça um sistema para substituição de backups, reutilizando os backups mais antigos primeiro. Use datas de expiração nos backups para evitar a substituição prematura.
- Rotule a mídia dos backups para identificar os dados e evitar a substituição de backups críticos.

  Use utilitários do SQL Server para fazer o backup do banco de dados:

- Transact-SQL
- SQL Distributed Management Objects
- Assistente para criar backup do banco de dados
- SQL Server Management Studio

Fazer backup de arquivos do servidor

Faça o backup e proteja os dados do sistema, da mesma forma como protege todos os ativos de valor em sua organização.

Convém executar esse procedimento à noite.

1 Faça o seguinte para parar o Adobe Connect:

a Selecione Iniciar > Programas > Adobe Connect Server > Parar o Connect Central Service.

b Selecione Iniciar > Programas > Adobe Connect Server > Parar o Connect Meeting Service.

2 Faça uma cópia de backup do diretório de conteúdo.

O local padrão é C:\breeze.

3 Faça uma cópia de backup do arquivo custom.ini.

O local padrão é C:\breeze\.

4 Faça o seguinte para iniciar o Adobe Connect:

a Selecione Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Meeting Service.

b Selecione Iniciar > Programas > Adobe Connect Server > Iniciar o Connect Central Service.

Fazer backup do banco de dados

Para fazer backup de qualquer edição do Microsoft SQL Server, você pode usar o Microsoft SQL Server Management Studio ou a janela Prompt de Comando.

A edição do SQL Server instalada com o Adobe Connect Server não inclui o SQL Server Management Studio. Contudo, você pode baixar o Microsoft SQL Server Management Studio Express da Microsoft.

Usar o SQL Server Management Studio para fazer backup do SQL Server

Importante: *Não desinstale o banco de dados.*

1 No Windows, selecione Iniciar > Programas > Microsoft SQL Server 2005 > SQL Server Management Studio.

2 No painel de árvore da janela do Object Explorer, clique com o botão direito do mouse no banco de dados (chamado "breeze", por padrão) e escolha Tarefas > Backup.

Nota: *Para obter instruções completas sobre backup e recuperação do banco de dados do SQL Server, consulte o site de suporte da Microsoft.*

Usar a janela Prompt de Comando para fazer backup do SQL Server

Para acessar as informações de ajuda dos comandos do banco de dados, digite `osql ?` no prompt do DOS e pressione Enter.

Importante: *Não desinstale o banco de dados.*

1 Faça logon no servidor que hospeda o Adobe Connect Server.

2 Crie uma pasta para armazenar os arquivos de backup do banco de dados.

Este exemplo usa a pasta c:\Connect_Database.

3 Selecione Iniciar > Executar e digite **cmd** na caixa Abrir. Clique em OK.

4 Ao receber o prompt, mude para o diretório onde você instalou o banco de dados. Por padrão, o diretório é C:\Arquivos de Programas\Microsoft SQL Server\90\Tools\Binn.

5 No prompt, digite **osql -E** para fazer logon no mecanismo de banco de dados e pressione Enter.

6 Digite **BACKUP DATABASE nome-do-banco-de-dados TO DISK = 'C:\Connect_Database\nome-do-banco-de-dados.bak'** para executar um utilitário do Microsoft SQL que faz o backup do banco de dados do Connect e pressione Enter.

O nome padrão do banco de dados é *breeze* .

7 No prompt, digite **go** e pressione Enter.

A janela de comando exibe mensagens relacionadas ao backup.

8 No prompt, digite **quit** e pressione Enter.

9 Para verificar se o backup foi realizado com êxito, verifique se há um arquivo breeze.bak no diretório c:\Connect_Database.

10 Para reiniciar o banco de dados, na área de trabalho do Windows, selecione Iniciar > Painel de controle > Ferramentas administrativas > Serviços. Na janela Serviços, clique com o botão direito do mouse em SQL Server (MSSQLSERVER) e selecione Iniciar no menu de contexto.

Criação de relatórios personalizados

Criação de relatórios personalizados a partir de exibições de esquema em estrela

O Adobe Connect usa um banco de dados para armazenar informações sobre usuários, conteúdo, cursos e reuniões. A atividade dos usuários preenche o banco de dados. Você pode usar ferramentas como o Adobe® ColdFusion® Studio e o Business Objects Crystal Reports para consultar exibições de esquema em estrela e exibir os dados. Você também pode usar ferramentas baseadas em SQL, como o SQL Query Analyzer.

Os aplicativos do Adobe Connect a seguir podem produzir dados para relatórios:

Adobe Connect Meeting Comparecimento à reunião, duração da reunião e conteúdo da reunião.

Adobe Presenter Exibições de conteúdo, de slides e de apresentações.

Adobe Connect Training Informações para gerenciamento de cursos, como estatísticas de comparecimento ao curso, estatísticas de exibição do conteúdo e resultados de testes.

Nota: *Além disso, você pode executar relatórios no aplicativo da Web Adobe Connect Central e exibi-los ou baixá-los em formato CSV. Para obter mais informações, consulte Geração de relatórios no Connect Central.*

Fato de SCO

Coluna	Descrição
dim_sco_details_sco_id	ID do SCO
dim_sco_details_sco_version	Versão do SCO
max_retries	Número máximo de tentativas
owner_user_id	ID de usuário do proprietário do SCO
disk_usage_kb	Uso do disco em quilobytes
passing_score	Pontuação para aprovação
max_possible_score	Pontuação máxima possível
views	Número de exibições
unique_viewers	Número de usuários que exibiram a SCO pelo menos uma vez
slides	Número de slides
questions	Número de perguntas
max_score	Pontuação máxima
min_score	Pontuação mínima
average_score	Pontuação média
average_passing_score	Pontuação média para aprovação
total_registered	Pontuação média para reprovação
total_participants	Total de usuários registrados
account_id	Total de participantes

Dimensão de detalhes de SCO

Coluna	Descrição
sco_id	ID do SCO
sco_version	Versão do SCO
sco_name	Nome
sco_description	Descrição
sco_type	Tipo de SCO
sco_int_type	Tipo de número inteiro
is_content	O SCO é de conteúdo?
url	URL
parent_name	Nome do SCO pai
parent_sco_id	ID do SCO pai
parent_type	Tipo de SCO pai
date_sco_created	Data de criação
date_sco_modified	Data de modificação
sco_start_date	Data de início
sco_end_date	Data de término
version_start_date	Data de início da versão
version_end_date	Data de término da versão
sco_tag_id	ID da tag
passing_score	Pontuação para aprovação
max_possible_score	Pontuação máxima possível
linked_sco_id	Id de um SCO vinculado
linked_type	Tipo de um SCO vinculado
owner_user_id	ID do usuário proprietário
storage_bytes_kb	Bytes de armazenamento em quilobytes
account_id	Id da conta

Fato de atividade

Coluna	Descrição
dim_activity_details_activity_id	Id da atividade
score	Pontuação
passed	Aprovado
completed	Concluído
peak_session_users	Número máximo de usuários por sessão

Coluna	Descrição
number_correct	Número de respostas corretas
number_incorrect	Número de respostas incorretas
number_of_questions	Número de perguntas
number_of_responses	Número de respostas
account_id	Id da conta

Dimensão de detalhes de atividade

Coluna	Descrição
activity_id	Id da atividade
dim_sco_details_sco_id	ID do SCO
dim_sco_details_sco_version	Versão do SCO
dim_users_user_id	ID do usuário
dim_sco_details_parent_sco_id	Id do SCO pai
score	Pontuação
passed	Aprovado
completed	Concluído
activity_type	Tipo de atividade
role	Função
date_activity_started	Data de início
date_activity_finished	Data de término
dim_cost_center_id	Id do centro de custo
cost_center_audit_id	Id da auditoria
session_start_date	Data de início da sessão
session_end_date	Data de término da sessão
attendance_activity	O comparecimento é uma atividade?
session_id	ID da sessão
account_id	Id da conta

Dimensão de testes finais de currículo

Coluna	Descrição
dim_sco_details_curriculum_sco_id	Id do currículo
dim_sco_details_curriculum_sco_version	Versão do currículo
test_out_subject_sco_id	ID do SCO de assunto
test_out_target_sco_id	ID do SCO de meta
test_out_type	Tipo de teste final

Coluna	Descrição
account_id	Id da conta

Dimensão de pré-requisitos de currículo

Coluna	Descrição
dim_sco_details_curriculum_sco_id	Id do currículo
dim_sco_details_curriculum_sco_version	Versão do currículo
pre_requisite_subject_sco_id	ID do SCO de assunto
pre_requisite_target_sco_id	ID do SCO de meta
pre_requisite_type	Tipo de pré-requisito
account_id	Id da conta

Dimensão de requisitos para conclusão de currículo

Coluna	Descrição
dim_sco_details_curriculum_sco_id	Id do currículo
dim_sco_details_curriculum_sco_version	Versão do currículo
completion_subject_sco_id	ID do SCO de assunto
completion_target_sco_id	ID do SCO de meta
completion_requirement_type	Tipo de requisito para conclusão
account_id	Id da conta

Fato de exibições de slide

Coluna	Descrição
dim_slide_view_details_slide_view_id	ID de exibição de slides
dim_activity_details_activity_id	Id da atividade
slide_view_display_sequence	Seqüência de exibição
account_id	Id da conta

Dimensão de detalhes de exibições de slides

Coluna	Descrição
slide_view_id	ID de exibição de slides
date_slide_viewed	Data de exibição do slide
slide_name	Nome do slide
slide_description	Descrição do slide
account_id	Id da conta

Fato de respostas

Coluna	Descrição
dim_answer_details_answer_id	Id da resposta
dim_activity_details_activity_id	Id da atividade
dim_question_details_question_id	ID da pergunta
answer_display_sequence	Seqüência de exibição
answer_score	Pontuação?
answer_correct	Está correto?
account_id	Id da conta

Dimensão de detalhes de resposta

Coluna	Descrição
answer_id	Id da resposta
date_answered	Data da resposta
resposta	Resposta
account_id	Id da conta

Fato de pergunta

Coluna	Descrição
dim_sco_details_sco_id	ID do SCO
dim_sco_details_sco_version	Versão do SCO
dim_question_details_question_id	ID da pergunta
number_correct	Número de respostas corretas
number_incorrect	Número de respostas incorretas
total_responses	Total de respostas
high_score	Pontuação alta
low_score	Pontuação baixa
average_score	Pontuação média
account_id	ID da conta

Dimensão de detalhes de pergunta

Coluna	Descrição
question_id	ID da pergunta
question_display_sequence	Seqüência de exibição
question_description	Descrição
question_type	Tipo de pergunta

Coluna	Descrição
account_id	ID da conta

Dimensão de respostas a perguntas

Coluna	Descrição
dim_question_details_question_id	ID da pergunta
response_display_sequence	Seqüência de exibição das respostas
response_value	Valor
response_description	Descrição
account_id	ID da conta

Dimensão de grupos

Coluna	Descrição
group_id	Id do grupo
group_name	Nome do grupo
group_description	Descrição do grupo
group_type	Tipo de grupo
account_id	ID da conta

Dimensão de grupos de usuários

Coluna	Descrição
user_id	ID do usuário
group_id	Id do grupo
group_name	Nome do grupo
account_id	ID da conta

Dimensão de usuário

Coluna	Descrição
user_id	ID do usuário
logon	Logon
first_name	Nome
last_name	Sobrenome
email	Endereço de email
user_description	Descrição do usuário
user_type	Tipo de usuário
most_recent_session	Data da sessão mais recente

Coluna	Descrição
session_status	Status da sessão
manager_name	Nome do gerente
disabled	Desativado
account_id	ID da conta
custom_field_1	Valor do campo personalizado 1
custom_field_2	Valor do campo personalizado 2
custom_field_3	Valor do campo personalizado 3
custom_field_4	Valor do campo personalizado 4
custom_field_5	Valor do campo personalizado 5
custom_field_6	Valor do campo personalizado 6
custom_field_7	Valor do campo personalizado 7
custom_field_8	Valor do campo personalizado 8
custom_field_9	Valor do campo personalizado 9
custom_field_10	Valor do campo personalizado 10

Dimensão de nomes de campos personalizados

Coluna	Descrição
dim_column_name	Nome da coluna de campos personalizados
custom_field_name	Nome do campo personalizado
account_id	ID da conta

Dimensão de centros de custo

Coluna	Descrição
cost_center_id	Id do centro de custo
cost_center_name	Nome do centro de custo
cost_center_description	Descrição do centro de custo

Criação de relatórios personalizados a partir de exibições herdadas

Nota: *O Connect versão 7 introduziu exibições de esquema em estrela que você pode consultar para criar relatórios personalizados. Ainda há suporte às exibições de banco de dados herdadas, mas as exibições de esquema em estrela são mais padronizadas e robustas.*

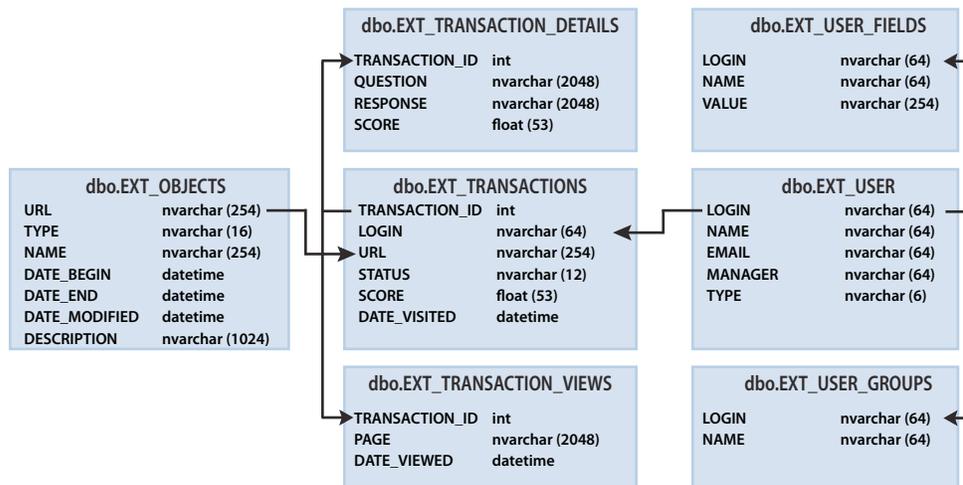
O Adobe Connect usa um banco de dados para armazenar informações sobre usuários, conteúdo, cursos e reuniões. A atividade dos usuários preenche o banco de dados. Você pode usar ferramentas como o Business Objects Crystal Reports para consultar o banco de dados e exibir os dados. Você também pode usar ferramentas baseadas em SQL, como o SQL Query Analyzer.

Os aplicativos do Adobe Connect a seguir podem produzir dados para relatórios:

Connect Meeting Comparecimento à reunião, duração da reunião e conteúdo da reunião.

Adobe Presenter Exibições de conteúdo, de slides e de apresentações.

Connect Training Informações para gerenciamento de cursos, como estatísticas de comparecimento ao curso, estatísticas de exibição do conteúdo e resultados de testes.

Exibir relacionamentos entre exibições do banco de dados

As setas representam os relações entre entidades entre as sete exibições de relatório.

Nota: *Não há suporte para exibições que não sejam identificadas neste documento, alteração de exibições que não sejam identificadas neste documento ou acesso direto ao esquema de banco de dados subjacente.*

❖ Use uma ferramenta de diagramação que se conecte ao seu banco de dados para ver as relações entre as exibições do banco de dados.

EXT_TRANSACTIONS

Uma ID de transação exclusiva é gerada cada vez que um usuário interage com um objeto. A exibição EXT_TRANSACTIONS retorna os dados listados na seguinte tabela:

Coluna	Tipo de dado	Descrição
TRANSACTION_ID	INT	ID exclusiva dessa transação.
LOGIN	NVARCHAR	Nome do usuário que realizou a transação.
URL	NVARCHAR	Objeto com que o usuário interagiu.
STATUS	NVARCHAR	Pode ser aprovado, reprovado, concluído ou em andamento.
SCORE	FLOAT	A pontuação do usuário.
DATE_VISITED	DATETIME	Data em que esta transação foi feita ou exibida.

Exemplo de consulta e dados A consulta a seguir retorna os dados na seguinte tabela:

```
select * from ext_transactions where url = '/p63725398/' order by login, date_visited asc;
```

TRANSACTION_ID	LOGIN	URL	STATUS	SCORE	DATE_VISITED
10687	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:56:16.500
10688	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:56:16.500
10693	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	0.0	2006-12-15 00:58:23.920
10714	test1-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:09:20.810
10698	test2-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:00:49.483
10723	test3-lnagaraj@test.enang.com	/p63725398/	in-progress	10.0	2006-12-15 01:11:32.153
10729	test3-lnagaraj@test.enang.com	/p63725398/	concluído	20.0	2006-12-15 01:12:09.700

Notas de consulta A exibição EXT_TRANSACTIONS retorna todas as transações existentes para um determinado usuário e uma determinada sessão de treinamento. Para ver a transação mais recente, verifique o valor DATE_VISITED máximo.

É possível filtrar pelos campos STATUS e URL para obter uma lista de usuários aprovados em uma sessão de treinamento específica:

```
select * from ext_transactions where url = '/p31102136/' and status = 'user-passed' order by
login, date_visited asc;
```

Geração de dados Ações de usuário que geram dados nesta exibição:

- Participação em uma reunião
- Exibição de um conteúdo
- Participação em uma sessão de treinamento (curso ou currículo)

Dados excluídos •Número do certificado, que não existe no banco de dados

- Pontuação máxima, geralmente não disponível

EXT_TRANSACTIONS_VIEWS

A exibição EXT_TRANSACTIONS_VIEWS recupera dados sobre os slides ou páginas exibidos pelos usuários.

Coluna	Tipo de dado	Descrição
TRANSACTION_ID	INT	ID exclusiva desta transação (pode ser mesclada com TRANSACTION_DETAILS para resumir por URL).
PAGE	NVARCHAR	Número do slide ou página exibida.
DATE_VIEWED	DATETIME	Data desta exibição.

Exemplo de consulta e dados A consulta a seguir retorna os dados na seguinte tabela:

```
select * from ext_transaction_views where transaction_id = 10702 order by page asc;
```

TRANSACTION_ID	PAGE	DATE_VISITED
10702	0	2006-12-15 01:01:13.153
10702	1	2006-12-15 01:01:18.233
10702	2	2006-12-15 01:01:59.840
10702	3	2006-12-15 01:02:20.717

Geração de dados A data é gerada nesta exibição sempre que um usuário exibe um conteúdo ou uma sessão de treinamento.

EXT_USERS

A exibição EXT_USERS lista os usuários e os atributos de perfil associados:

Coluna	Tipo de dado	Descrição
LOGIN	NVARCHAR	Identificador exclusivo do usuário.
NAME	NVARCHAR	Nome exclusivo do usuário.
EMAIL	NVARCHAR	Endereço de email exclusivo.
MANAGER	NVARCHAR	O logon do gerente. O gerente é sempre definido como NULL.
TYPE	NVARCHAR	Usuário ou convidado. O tipo é sempre definido como usuário.

Exemplo de consulta e dados A consulta a seguir retorna os dados na seguinte tabela:

```
select * from ext_users;
```

LOGIN	NAME	EMAIL	MANAGER	TYPE
test4-lnagaraj@test.enang.com	test4 laxmi	test4-lnagaraj@test.enang.com	NULL	user
test7-lnagaraj@test.enang.com	TEST7 laxmi	test7-lnagaraj@test.enang.com	NULL	user

Geração de dados Os dados são atualizados nesta exibição sempre que um convidado ou usuário é criado, atualizado ou excluído.

Dados excluídos •Senha, que não é armazenada em texto simples.

- Fuso horário e idioma, que não ficam disponíveis na forma legível por humanos. Por exemplo, PST é 323.
- Último logon, que consome recursos demais para ser calculado. Em vez disso, use uma consulta `max(date_visited)` a partir da exibição EXT_TRANSACTIONS para recuperar esses dados.
- Sessão ativa, que são dados da exibição EXT_TRANSACTION. Em vez disso, use uma consulta `STATUS='IN-PROGRESS'` para recuperar esses dados.
- Os usuários excluídos não aparecem na exibição EXT_USERS. Os usuários excluídos continuam aparecendo na exibição EXT_TRANSACTION.
- Os dados sobre grupos não são incluídos nesta exibição.
- Dados sobre campos personalizados predefinidos pelo usuário. Essas informações estão disponíveis para cada usuário na exibição EXT_USER_FIELDS.

EXT_USER_FIELDS

A exibição EXT_USER_FIELDS lista campos personalizados novos e predefinidos para um usuário específico. Ela também lista campos personalizados para usuários convertidos em convidados.

Coluna	Tipo de dado	Descrição
LOGIN	NVARCHAR	Identificador exclusivo do usuário.
NAME	NVARCHAR	Nome do campo, como número de telefone.
VALUE	NVARCHAR	Valor do campo, como 415.555.1212.

Exemplo de consulta e dados A consulta a seguir retorna os dados na seguinte tabela:

```
select * from ext_user_fields where login = 'test4-lnagaraj@test.enang.com';
```

LOGIN	NAME	VALUE
test4-lnagaraj@test.enang.com	{e-mail}	test4-lnagaraj@test.enang.com
test4-lnagaraj@test.enang.com	{first-name}	test4
test4-lnagaraj@test.enang.com	{last-name}	laxmi
test4-lnagaraj@test.enang.com	{x-job-title}	sw engr 4
test4-lnagaraj@test.enang.com	{x-direct-phone}	NULL
test4-lnagaraj@test.enang.com	{x-direct-phone-key}	NULL
test4-lnagaraj@test.enang.com	SSN	777

Geração de dados Ações que geram dados nesta exibição: adicionar, criar ou atualizar campos personalizados novos ou predefinidos para um ou mais usuários.

EXT_USER_GROUPS

A exibição EXT_USER_GROUPS lista dados sobre grupos e os membros a eles associados. A exibição EXT_USER_GROUPS usa os dados listados na tabela a seguir:

Coluna	Tipo de dado	Descrição
LOGIN	NVARCHAR	Nome do usuário.
NAME	NVARCHAR	Nome do grupo.

Exemplo de consulta e dados A consulta a seguir retorna os dados na seguinte tabela:

```
select * from ext_user_groups where login = 'lnagaraj@adobe.com';
```

LOGIN	NAME
lnagaraj@adobe.com	{admins}
lnagaraj@adobe.com	{authors}
lnagaraj@adobe.com	{everyone}
lnagaraj@adobe.com	Laxmi Nagarajan

Notas de consulta Há suporte para o aninhamento de vários grupos na versão 5.1 e posteriores. Por exemplo, se o grupo A contiver o grupo B, e você estiver no grupo B, você estará listado como membro de A.

Grupos incorporados, como o grupo Administradores, usam nomes de código no esquema, como nesta consulta SQL: `SELECT * FROM EXT_USER_GROUPS where group='{admins}`. O nome de código distingue os grupos incorporados dos grupos definidos pelo usuário.

Geração de dados Ações de usuário que geram dados nesta exibição:

- Criação, atualização ou exclusão de um grupo
- Alteração da associação de um grupo

EXT_OBJECTS

A exibição EXT_OBJECTS lista todos os objetos do sistema (como reuniões, conteúdo, cursos etc.) e seus atributos.

Coluna	Tipo de dado	Descrição
URL	NVARCHAR	Identificador exclusivo do objeto.
TYPE	NVARCHAR	Seja apresentação, curso, arquivo FLV, arquivo SWF, imagem, arquivamento, reunião, currículo, pasta ou evento
NAME	NVARCHAR	Nome do objeto como aparece na lista de conteúdo.
DATE_BEGIN	DATETIME	A data em que o objeto está programado para iniciar.
DATE_END	DATETIME	A data em que o objeto está programado para terminar.
DATE_MODIFIED	DATETIME	A data em que o objeto foi modificado.
DESCRIPTION	NVARCHAR	Informações de resumo do objeto inseridas durante a criação de uma reunião, um conteúdo, um curso ou outro tipo de objeto.

Exemplo de consulta e dados A consulta SQL a seguir retorna os dados da seguinte tabela:

```
select * from ext_objects order by type asc;
```

URL	TYPE	NAME	DATE_BEGIN	DATE_END	DATE_MODIFIED	DESCRIPTION
/p79616987/	course	test api	2006-12-08 23:30:00.000	NULL	2006-12-08 23:36:55.483	NULL
/p47273753/	curriculum	test review curric	2006-12-14 21:00:00.000	NULL	2006-12-14 21:00:30.060	NULL
/tz1/	meeting	{default-template}	2006-12-12 19:15:00.000	2006-12-12 20:15:00.000	2006-12-12 19:25:07.750	release presentation
/p59795005/	presentation	ln-QUIZ-TEST1	NULL	NULL	2006-12-15 00:43:19.797	managers meeting

Notas de consulta Você pode obter todos os objetos de um tipo específico filtrando pelo campo TYPE. Por exemplo, a consulta SQL a seguir filtra cursos e currículos:

```
select * from ext_objects where type in ('course', 'curriculum');
```

Use a seguinte consulta SQL para retornar uma lista dos tipos disponíveis no sistema:

```
select DISTINCT (type) from ext_objects;
```

Geração de dados Ações de usuário que geram dados nesta exibição:

- Criação ou atualização de uma reunião, curso ou currículo

- Carregamento ou atualização de conteúdo

Dados excluídos •Duração, que pode ser calculada com `date_end - date_begin`.

- Tamanho do disco, que expõe regras comerciais em relação a cópias e originais
- ID da pasta
- Objetos excluídos não aparecem na exibição EXT_OBJECTS. Objetos excluídos continuam existindo na exibição EXT_TRANSACTION.